



COLONIALISMO DIGITAL

análisis de la agenda comercial europea

✉ **Suscribirse a nuestro boletín:**
www.tni.org/es/suscribirse

o escanear el código QR:



AUTORAS: Sofia Scasserra y Carolina Martínez Elebi

EDICIÓN: Nick Buxton

DISEÑO: Evan Clayburg

Publicado por Transnational Institute, Amsterdam, Julio 2021

AGRADECIMIENTOS: Nos gustaría dar las gracias por los valiosos comentarios al texto a Adriana Foronda, Pablo Sanchez Centellas, Nick Buxton y Cecilia Olivet.

El contenido de este informe se puede citar o reproducir con fines no comerciales y siempre que se mencione debidamente la fuente de información. El TNI agradecería recibir una copia o un enlace del texto en que se utilice o se cite este documento.

ÍNDICE

Resumen Ejecutivo	1
1- Introducción	3
2- ¿Qué cláusulas contienen los capítulos de comercio digital?.....	7
3- La política de la UE en comercio digital.....	10
4- Las consecuencias de la política de comercio digital de la UE para el Surglobal	15
5- Conclusiones.....	18
Anexo: Las cláusulas de comercio digital y sus efectos	22

RESUMEN EJECUTIVO

La batalla mundial por el control de la economía digital suele describirse como una lucha entre dos únicos titanes: EE.UU. y China, pero eso no significa que la UE se haya quedado parada. Como se documenta en este informe, la UE ha hecho grandes esfuerzos por ponerse al día utilizando las negociaciones y las normas comerciales para hacer valer sus propios intereses. En el proceso, la UE está tratando de trepar sobre las espaldas de los países en desarrollo, socavando la posibilidad de que todos compartan equitativamente los beneficios del desarrollo tecnológico.

Este informe examina 14 cláusulas sobre comercio digital que la UE defiende en sus negociaciones comerciales y su impacto en los países en desarrollo. A partir de un análisis exhaustivo de 13 acuerdos de libre comercio de la UE, así como de su posicionamiento en la Organización Mundial del Comercio, muestra que la UE ha adoptado una estrategia colonialista, saliendo a la caza de datos del Sur global, para posicionar a sus propias empresas en las nuevas cadenas de valor cibernéticas globales. Para empoderar a sus propias corporaciones tecnológicas, la UE está tratando de imponer cláusulas en las negociaciones comerciales que obstaculizarán la industrialización digital, restringirán la necesaria supervisión estatal de las empresas y socavarán los derechos de los ciudadanos en otros lugares, en particular en los países en desarrollo. Aunque estas cláusulas son de naturaleza técnica y obtusas para el público en general, pueden afectar a todo, incluidos los derechos de las personas a la privacidad, la naturaleza y el funcionamiento de los servicios públicos, la posibilidad de desarrollo económico e industrialización, la responsabilidad del gobierno, incluso la calidad de la propia democracia.

CLÁUSULAS COMERCIALES DIGITALES

1. Medidas que obstaculizan la industrialización digital
 - a. [Transferencia transfronteriza de datos](#)
 - b. [Prohibición de la localización de datos](#)
 - c. [Prohibición del tratamiento local de datos](#)
 - d. [No divulgación del código fuente de los programas informáticos y de los algoritmos correspondientes](#)
 - e. [Eliminación de los derechos de aduana sobre los productos digitales y/o las transmisiones electrónicas](#)
 - f. [Contratación pública electrónica](#)
2. Medidas que restringen la necesaria supervisión estatal de las empresas
 - g. [Autorización previa](#)
 - h. [No discriminación de los productos digitales](#)
 - i. [Autenticación y firmas electrónicas](#)
 - j. [Vigilancia](#)
 - k. [Responsabilidad de los proveedores de servicios intermediarios](#)
3. Medidas que afectan a los derechos de los ciudadanos en línea
 - l. [Protección de datos personales](#)
 - m. [Protección del consumidor en línea](#)

La batalla que libran la UE, Estados Unidos y China es por el control de los datos que generamos cada vez que nos conectamos a internet como materia prima básica para su proceso de producción. El verdadero valor no reside en los datos en sí, sino en el procesamiento de los mismos para ofrecer y vender explicaciones algorítmicas del comportamiento humano.

El informe muestra que la UE fue inicialmente lenta en el avance de su agenda de comercio digital, pero ha sido mucho más agresiva desde 2016. La UE parece tener dos objetivos. En primer lugar, convertirse en un actor digital mundial mediante la creación de normas que respalden la transición de sus industrias hacia la digitalización y que, a continuación, fijen su dominio a largo plazo. Esto incluye campos tan diversos como los recursos humanos, la logística, los servicios médicos, el entretenimiento, la educación y el transporte urbano inteligente, aunque el empuje más poderoso proviene de la industria automovilística de la UE, deseosa de dominar los vehículos autónomos e inteligentes del futuro. En segundo lugar, y sobre todo en el marco de las negociaciones de la OMC, la UE parece dispuesta a postrarse ante el poder de los gigantes digitales estadounidenses, conocidos como GAFAM (Google, Apple, Facebook, Amazon y Microsoft), que han gastado una fortuna en grupos de presión y han conseguido dar forma a cualquier negociación que incluya normas sobre la economía digital.

La UE ya ha firmado seis acuerdos que incluyen cláusulas sobre comercio digital, con Canadá, Singapur, Vietnam, Mercosur, Japón y México. Actualmente está negociando otros siete acuerdos que incluyen cláusulas relacionadas con lo digital con Túnez, Chile, Indonesia, Australia, Nueva Zelanda y la región de África Oriental y Meridional (ESA), y a nivel internacional en la Organización Mundial del Comercio. Las negociaciones en curso con Indonesia, Australia, Nueva Zelanda y la región de África Oriental y Meridional (ESA), junto con la propuesta presentada por la UE a la Organización Mundial del Comercio, son las que incluyen las cláusulas más perjudiciales para los países del Sur global.

Las 14 normas comerciales resumidas en el recuadro están cuidadosamente diseñadas para garantizar que las grandes empresas tecnológicas de la UE y Estados Unidos puedan operar libremente y maximizar sus beneficios en la economía digital, al tiempo que restringen la capacidad de los Estados para regular el sector, redistribuir los beneficios, mejorar sus servicios públicos o llevar adelante una estrategia de desarrollo tecnológico local. También desfinancian al Estado, al prohibir la recaudación de impuestos sobre las transmisiones electrónicas, una enorme pérdida potencial en el futuro dada la transición de todo a la red.

Incluso en los casos en los que la UE se ha considerado un actor más progresista que China y Estados Unidos, como su adopción en 2018 del Reglamento General de Protección de Datos (RGPD), exportar esto por medio de normas comerciales afianzará, en lugar de socavar, un modelo extractivista. Esto se debe a que no va acompañado de los recursos necesarios para lograrlo, lo que, por lo tanto, crea costes adicionales para los países de bajos ingresos y una competencia desleal.

La agenda de comercio digital de la UE equivale a una agenda de extractivismo. Extraer la materia prima (los datos) del Sur global sin pagar nada por ella y llevarla a los países en los que están radicados para procesarla y volver a vendernos esa tecnología. También es una estrategia para el subdesarrollo estructural deliberado de los países de bajos ingresos, ya que pretende poner reglas que les impidan capitalizar los ingresos y beneficios potenciales del desarrollo tecnológico. Parafraseando al conocido economista del desarrollo Ha-Joon Chang, la agenda comercial de la UE está retirando la escalera digital del desarrollo.

Los perdedores en la batalla por la hegemonía tecnológica son los ciudadanos de a pie. Las normas comerciales no se están construyendo para fortalecer los derechos de los ciudadanos o la democracia, sino para beneficiar a las grandes tecnológicas, dándoles mercados y recursos de forma gratuita, monopolios ilimitados y sin responsabilidad social o fiscal. Contra este robo de recursos y el extractivismo digital, el único remedio es conservar la libertad de los Estados para regular, de modo que la gente pueda a su vez hacer valer su voluntad. Por lo tanto, es fundamental que los Estados se nieguen a firmar estos acuerdos como un primer paso hacia un proceso de industrialización y soberanía digital a largo plazo.

1- INTRODUCCIÓN



Parece que pasaron miles de años, pero no fue hace tanto que nuestras vidas no pasaban por Internet ni existía un registro en tiempo real de nuestras relaciones sociales ni de lo que hablábamos, comprábamos, compartíamos, trabajábamos o viajábamos.

La economía se volvió digital rápidamente, e indudablemente la pandemia del COVID-19 terminó de configurar un mundo *online* que se fusiona con la vida *offline*. Es que si algo logró la virtualidad, es pasar desapercibida al punto que ya ni siquiera la cuestionamos. La hemos naturalizado.

Lo cierto es que, en estas últimas décadas, el capitalismo comenzó a mutar hacia una nueva fase como resultado de estas transformaciones: el capitalismo cibernético¹. Esta forma eficiente de capital que lentamente se fagocita a las formas tradicionales. Así, encontramos que en cada sector de la economía existe una versión cibernética o digital de ese producto o servicio, que termina ganando mercado y desplazando a las formas tradicionales de producción. Plataformas de delivery dominan el negocio de entregas por sobre los repartidores tradicionales. Spotify determina las reglas de mercado de la música. Shippo organiza la logística transnacional. Hasta el capital financiero encuentra un embrionario desarrollo cibernético a través de las criptomonedas.

Este capitalismo cibernético toma a los datos que generamos cada vez que nos conectamos a Internet como la materia prima fundamental para producir². El verdadero valor del ciber capitalismo -que genera ganancias extraordinarias a las empresas de tecnología- no está en esos datos. Al igual que en cualquier otro sistema productivo, la materia prima es básica, pero no salen de ahí las grandes ganancias. **Las ganancias provienen del procesamiento de esos datos para entregar y vender explicaciones algorítmicas sobre la conducta humana**³. En efecto, los trabajadores del sector de tecnología programan algoritmos que puedan procesar en tiempo real esos datos y entregar o vender el producto final a otras empresas. ¿Cuál es ese producto? La predicción o explicación de nuestro comportamiento y nuestras conductas. Ese es el verdadero valor de la economía del futuro. Procesar los datos para lograr obtener lo que algunos autores llaman el "excedente conductual"⁴. Este excedente conductual no es otra cosa que, primero, vender nuestro comportamiento como consumidores; luego, en una segunda etapa, vender nuestro comportamiento como ciudadanos; y, en la actualidad, en una nueva fase de este capitalismo cibernético, vender y procesar nuestra conducta como trabajadores.

¿Quiénes venden? ¿Quiénes procesan? ¿Quiénes programan? Son las grandes empresas de tecnología, conocidas popularmente como GAFAM (Google, Apple, Facebook, Amazon y Microsoft entre otras). Estas empresas comenzaron a acumular datos a partir del desarrollo de diversas plataformas tecnológicas y son las que hoy determinan las reglas de juego de la economía digital. Todas empresas norteamericanas, cuyos únicos competidores globales que pueden pelearles el liderazgo son las empresas tecnológicas de China, como Alibaba o Tencent por mencionar algunas.

Esta economía digital avanza en todos los sectores y en todas las regiones del mundo. La venta en línea gana terreno por sobre la venta física; la televisión tradicional -por aire o cable- pierde la batalla contra plataformas de contenidos como YouTube o Netflix; la educación en línea o la telemedicina se desarrollan cada vez más y se consolidan como nuevas formas de acercarse a servicios esenciales. A medida que nos conectemos más a Internet en situaciones cotidianas, las empresas pasarán inadvertidas en esta succión de datos, y podrán saber nuestros comportamientos y preferencias. El diseño de publicidad y de estrategias elaboradas a través de la economía del comportamiento prescriben y prescribirán la realidad que vivimos. Si un algoritmo toma decisiones sobre nuestras vidas a base de toda la información que tiene de nosotros, tiene el poder de predecirlo y condicionar nuestro comportamiento.

Esta realidad, que bien puede parecer ciencia ficción, ya está ocurriendo y se va a intensificar y profundizar aún más con la llegada de la red 5G y el Internet de las Cosas (IoT), donde una inmensidad de dispositivos y sensores serán conectados a la red, teniendo hogares inteligentes que nos vigilan 24/7. La heladera sabrá nuestros gustos y podrá recomendarnos compras y ofertas, avisarnos cuando se están por vencer los productos o si nos estamos por quedar sin leche y hasta indicarnos que no es sano comer determinada manteca; el aire acondicionado podrá saber a qué temperatura nos resulta agradable el ambiente y programarse para que, cuando lleguemos, todo esté maravillosamente dispuesto y hasta sugerirnos cambiar esa temperatura acorde a las recomendaciones de consumo eléctrico. Pero también podrán exigirnos pagos adicionales para brindar el servicio, o acceder a nuestros dispositivos de manera remota en caso de que nuestro comportamiento no sea acorde a sus intereses. Una empresa aseguradora de autos podría pedir que nuestro vehículo quede inmovilizado si no tenemos una conducta acorde al estándar que esperan de nosotros, por ejemplo, o si tenemos deuda acumulada con dicha aseguradora.

Este capitalismo cibernético llegó para quedarse. Existe un modelo que se vislumbra de vigilancia masiva, pero también de subdesarrollo estructural para la mayor cantidad de países del planeta. La extracción de datos y el desarrollo tecnológico se está dando, fundamentalmente, en dos países y por un puñado de empresas. Llevan adelante prácticas extractivistas ya conocidas por la historia de la humanidad, absorbiendo materia prima (datos) del sur global sin pagar nada a cambio y llevándola a sus países para procesarla y vendernos esa tecnología. Esta historia no es nueva y bien puede emular al proceso vivido en la conquista de América con la plata del extraída de Potosí, o a la venta de materias primas para la agroindustria desde América Latina o África para ser procesadas en otros lugares y sus productos poder ser revendidos. Un sistema que debilita los términos de intercambio y somete al empobrecimiento a regiones enteras del mundo. Mientras este proceso es liderado por China y EEUU, todos los demás países miran atónitos una tecnología que es difícil de comprender y que recién ahora descubrimos el daño potencial que puede hacer a nuestras economías y democracias. En efecto, la distribución masiva de noticias falsas, escándalos como el de Cambridge Analytica⁵ o la ya probada manipulación⁶ de votantes por parte de Facebook los días de elecciones⁷, muestran cómo nuestros sistemas políticos pueden ser vulnerados desde afuera por empresas que no deberían tener ninguna influencia en el destino de los pueblos.

No podemos renunciar al sueño del desarrollo. No podemos renunciar a la democracia. No podemos renunciar a la privacidad. Perderlas no es un destino inevitable. Existe otra manera de desarrollar tecnología y aprovechar sus beneficios para toda la sociedad. Hay modelos alternativos respetuosos de la privacidad⁸, que reparten los beneficios económicos⁹ entre los ciudadanos que producen los datos y a los cuales les afecta la tecnología. Existen formas de pensar un Estado con una lógica de datos como bienes comunes¹⁰, diseñando y desarrollando servicios públicos de calidad, más eficientes, económicamente sustentables y culturalmente soberanos. Pensar los datos como bienes privados susceptibles de ser procesados únicamente para la ganancia de grandes empresas es mercantilizar nuestra humanidad: nuestra geolocalización, nuestras comunicaciones, nuestra sociedad, nuestros movimientos, gustos y costumbres no pueden ser bienes para el lucro privado. Si los declaramos bienes comunes, los beneficios económicos se repartirán mejor en las sociedades y podríamos hacer participar a todos los involucrados en determinado data set en la política de privacidad que le corresponde y en la utilización de los mismos. Una comunidad debería tener derecho a decidir cómo, por qué y para qué quiere que se utilicen sus datos.

Las grandes empresas de tecnología saben que sus ganancias dependen de poder seguir extrayendo datos y por eso necesitan reglas para mantener su control. Necesitan reglas que afiancen un modelo de negocios que les permita ser los dueños del capital cibernético, que les garanticen el

monopolio eterno de ese excedente conductual. Reglas que les permitan eliminar competidores y auto establecerse como el único modelo tecnológico futuro. Esas reglas ya están escritas pero aún no han logrado ser aprobadas a nivel global. Podemos verlas en las negociaciones que tienen curso en la Organización Mundial de Comercio (OMC), pero también en algunos Tratados de Libre Comercio (TLC) que ya se han firmado, y otros que están siendo negociados actualmente.

Estas reglas están perfecta y cuidadosamente diseñadas para que las grandes empresas de tecnología puedan operar libremente en la economía digital, pero también para limitar el poder de los Estados en su capacidad de regular, redistribuir las ganancias generadas, mejorar sus servicios públicos, o encauzar una estrategia de desarrollo tecnológico local. Pero sobre todo eso y, además, las reglas buscan desfinanciar a los Estados, prohibiendo el cobro de impuestos a toda transmisión electrónica: si la economía del futuro es online, limitar el cobro de impuestos a ese tipo de transacciones es la mayor amenaza a los ingresos fiscales.

El galardonado economista Ha-Joon Chang nos advertía en el año 2002 que: “Los países ricos han «echado a patadas la escalera» al obligar a los países pobres a aplicar políticas de libre mercado y libre comercio. Los países ya establecidos no quieren que surjan más competidores a través de las políticas nacionalistas que ellos mismos utilizaron con éxito en el pasado”¹¹. Su cita hoy, nos invita a pensar si esta nueva agenda de liberalización no está tratando de retirar la escalera a la industrialización digital de los países en vías en desarrollo una vez más. La historia que se repite a si misma.

No sólo la agenda de comercio electrónico incluye cláusulas que afectan a la economía digital, sino que existen también acuerdos en finanzas y telecomunicaciones que regulan la transferencia de datos en el sector, así como también los servicios computacionales, pero esos no fueron incluidos en el presente estudio.

En un mundo que recién empieza a comprender la nueva economía digital y su importancia, los Estados más poderosos del mundo, influenciados por las grandes empresas de tecnología, han marcado la agenda de comercio, escribiendo reglas que, de aprobarse, marcarán el futuro de nuestras sociedades, nuestras conductas, y nuestras vidas.

Es fundamental conocer qué se negocia y por qué es importante. No podemos permitirnos la entrega de soberanía y de capacidad regulatoria en una economía que ha puesto en jaque nuestras economías, y sobre todo, nuestras democracias.



2- ¿QUÉ CLÁUSULAS CONTIENEN LOS CAPÍTULOS DE COMERCIO DIGITAL?

En medio de una disputa geopolítica por la primacía económica y el liderazgo en el desarrollo de Inteligencia Artificial (IA), comenzaron a negociarse, tímidamente, cláusulas mal llamadas de “comercio electrónico”. Las primeras conversaciones sobre el tema comenzaron en la OMC en el año 1998. Al principio, parecía ser un mero tema comercial sobre tarifas aduaneras de los bienes y servicios comercializados por internet. Pero, al ver las cláusulas que se negocian hoy día, queda claro que otras cosas están en juego. Las reglas de gobernanza de toda la economía digital se están definiendo en estos acuerdos.

Para empezar, es bueno saber que de acuerdo con la OMC, *“Exclusivamente a efectos del programa de trabajo, y sin perjuicio de su resultado, se entiende por «comercio electrónico» la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos»*¹². Es decir, casi todos los bienes y servicios que se producen en la economía presente y futura.

La ya clásica ideología de “regular para que no existan reglas” pasó a ser la visión imperante. Y mientras en diversos foros se cita el crecimiento desmesurado de las empresas tecnológicas como justificativo para regular y lograr una mejor distribución de las ganancias, el texto que se impulsa está hecho por y para las grandes empresas¹³. En efecto, son estas empresas las que han logrado, mediante lobbys, posicionar sus demandas en las negociaciones. Las reglas básicamente otorgan todos los derechos a las grandes empresas multinacionales, y sólo responsabilidad y obligaciones a los Estados. Pero, sobre todo, ponen esposas y limitan la capacidad regulatoria de los Estados para dirigir la economía digital hacia objetivos de desarrollo.

La Unión Europea comenzó más tarde que el resto de los países desarrollados a incorporar algunas cláusulas digitales y de protección y uso de datos a las negociaciones de acuerdos de libre comercio bilaterales y en el marco del comercio internacional a través de la OMC. Las propuestas iniciales de la UE buscaban dar un marco regulatorio al comercio digital, pero no incluían el tipo de cláusulas más agresivas a favor de las corporaciones que promocionaba los Estados Unidos (EEUU). Pero en 2015/2016 se evidencia un cambio de rumbo. La UE comienza a incorporar demandas que, hasta el momento, sólo promocionaba EEUU. ¿Por qué este cambio? ¿Por qué esta diferencia? ¿Es que la UE no sabe lo que negocia o es que busca favorecer a las GAFAM (Google, Apple, Facebook, Amazon y Microsoft)? Detrás de las negociaciones hay una intencionalidad de desarrollar servicios tecnológicos absorbiendo datos del sur global, como alguna vez absorbieron metales preciosos y otras materias primas. Extractivismo digital que acumule una masa crítica de datos que haga que la UE pueda entrar en la contienda global por el poder tecnológico a partir del desarrollo de nuevas tecnologías como autos autónomos dada la gran industria automotriz que tiene Europa, entre otras.

Asimismo, las empresas norteamericanas están haciendo un lobby desmesurado¹⁴ logrando que las normativas europeas no los perjudiquen en sus negocios. Las empresas de tecnología, con Google a la cabeza, han gastado fortunas para influenciar toda aquella negociación que incluya las reglas de economía digital y conseguir un set de reglas a nivel doméstico y en la OMC que perpetúe el monopolio tecnológico de las mismas¹⁵.

Las cláusulas contenidas en los acuerdos de economía digital que se están negociando a nivel bilateral por la Unión Europea y a nivel multilateral en la OMC, configuran las reglas de juego con las que se va a establecer el capitalismo cibernético a futuro. Estas reglas son el corazón del sistema y nos muestran los intereses que hay detrás, así como las dificultades que los países periféricos encontrarán a la hora de poder desarrollar una estrategia de industrialización digital.

Un análisis exhaustivo de las cláusulas más relevantes incluidas en los capítulos¹⁶ de “comercio electrónico” o “comercio digital” que negocia la UE en sus tratados de libre comercio (TLC) permite agruparlas en tres grandes categorías.

La primera columna es la más dañina en términos de desarrollo para los países del sur global. Busca afianzar un modelo extractivista y desfinanciar a los Estados, además de generar una competencia brutal contra desarrollos incipientes de tecnologías locales. La segunda columna contiene medidas que restringen la capacidad del Estado de controlar a las empresas que operan en internet y moldean el mercado digital, dándoles derechos a las corporaciones y quitándoles obligaciones. La tercera columna incluye medidas que intentan desproteger a ciudadanos y consumidores, sobre todo en el sur global al hacer exigencias sin traspaso de recursos. Son medidas que deslindan de responsabilidades a las corporaciones y afectan los derechos ciudadanos en entornos digitales.

Medidas contra la industrialización digital de los países del Sur global	Medidas que restringen el control del Estado a las empresas	Medidas que se relacionan con los derechos de la ciudadanía digital
<u>Transferencia transfronteriza de datos</u>	<u>Autorización previa</u>	<u>Protección de información personal</u>
<u>Prohibición de localización de datos</u>	<u>No discriminación contra productos digitales</u>	<u>Protección al consumidor en línea</u>
<u>Prohibición del procesamiento de datos en el país local</u>	<u>Autenticación electrónica y firmas electrónicas</u>	<u>Medidas contra las comunicaciones electrónicas comerciales no solicitadas (SPAM)</u>
<u>No divulgación del código fuente del software y algoritmos relacionados</u>	<u>Vigilancia</u>	
<u>Eliminación de aranceles aduaneros sobre productos digitales y/o transmisiones electrónicas</u>	<u>Responsabilidad de los proveedores de servicios intermediarios</u>	
<u>Contratación pública electrónica</u>		

Las medidas aquí mencionadas se encuentran explicadas una por una en un anexo exhaustivo que incluye el texto completo del artículo en cuestión, una explicación detallada de los debates en torno a la problemática que generan y ejemplos claros para poder dimensionar el potencial impacto que tendrían.



3- LA POLÍTICA DE LA UE EN COMERCIO DIGITAL

La Unión Europea ha concluido, hasta el momento, seis tratados de libre comercio que incluyen alguna de las cláusulas relevantes en materia digital. A su vez, se encuentra actualmente en siete negociaciones distintas sobre comercio digital con países de todas las regiones del mundo.

Sin embargo, no todos los tratados concluidos o en negociación incluyen las mismas cláusulas o demandas en materia de economía digital por parte de la UE (ver cuadro 1 y 2). Las mismas fueron variando con el correr de los años, en la medida en que se hacía más relevante para las empresas de tecnología delinear reglas de juego que favorezcan sus intereses comerciales y monopólicos, trazando una estrategia para perpetuarse como líderes indiscutidos de la revolución 4.0.

Los tratados de comercio digital concluidos

De un análisis de las cláusulas en los tratados concluidos por la UE al día de hoy podemos establecer que el Acuerdo con México y Japón son los más peligrosos en materia de economía digital, seguido por Mercosur.

CUADRO 1 - Acuerdos finalizados con cláusulas de comercio digital¹⁷

Cláusulas	Canadá ¹⁸	Singapur ¹⁹	Vietnam ²⁰	Mercosur ²¹	Japón ²²	México ²³
<u>Transferencia Transfronteriza de Datos</u>	NO	PARCIAL	NO	NO	PARCIAL	PARCIAL
<u>Prohibición de localización de datos</u>	NO	NO	NO	NO	NO	NO
<u>Prohibición de procesamiento de datos en el país</u>	NO	NO	NO	NO	NO	NO
<u>No divulgación del código fuente del software y algoritmos relacionados</u>	NO	NO	NO	NO	SÍ	SÍ
<u>Eliminación de impuestos aduaneros en productos digitales y/o transmisiones electrónicas</u>	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Autorización previa</u>	NO	NO	NO	SÍ	SÍ	SÍ
<u>No discriminación contra productos digitales</u>	NO	NO	NO	SÍ	SÍ	SÍ
<u>Autenticación y firmas electrónicas</u>	PARCIAL	PARCIAL	PARCIAL	SÍ	SÍ	SÍ
<u>Protección online del consumidor</u>	PARCIAL	PARCIAL	PARCIAL	SÍ	PARCIAL	SÍ
<u>Medidas contra comunicaciones electrónicas no solicitadas</u>	PARCIAL	PARCIAL	PARCIAL	SI	SI	SI
<u>Protección de datos personales y privacidad</u>	PARCIAL	PARCIAL	PARCIAL	NO	NO	NO
<u>Responsabilidad de los intermediarios</u>	PARCIAL	PARCIAL	PARCIAL	NO	NO	NO
<u>Compras públicas electrónicas</u>	NO	NO	SÍ	NO	NO	NO
<u>Vigilancia</u>	NO	NO	NO	NO	NO	NO
Año de comienzo de la negociación	2009	2010	2012	1999	2012	2016
Año en que se firmó el acuerdo (o en que concluyó la negociación).	2016	2018	2015	2019	2018	2018

Todas estas negociaciones comenzaron previo al 2016, y algunas, como las que sostuvo con el Mercosur, comenzaron en los años 90. Si hay algo que puede verse a simple vista es que la libre movilidad de datos, su localización, almacenamiento y procesamiento, no eran vistos como ejes estratégicos en ese momento. Esto explica por qué esas cláusulas no están en las agendas comerciales.

Inicialmente, la agenda digital consistía en mantener la moratoria de los derechos de aduana a las transmisiones electrónicas. A medida que se avanza en los años, se ve cómo más temas regulatorios se van metiendo en la agenda: la regulación del correo no deseado, la protección a los consumidores, las firmas electrónicas y las autorizaciones y licencias para operar. No obstante, no se ve una agenda digital tan agresiva como la de Estados Unidos todavía. EEUU tuvo una estrategia de colonialismo digital hacia los países en vías de desarrollo a través del extractivismo de datos desde, el comienzo de la revolución digital.

Es recién en las negociaciones con Japón y México, cuando se introduce el primer gran tema controversial, que es la no publicación del código fuente de los algoritmos. Lo curioso de los acuerdos que lo incluyen es ver cómo con el tiempo van sumando excepciones²⁴, a medida que se encuentran con impactos sociales problemáticos que pueden afectar la soberanía de los Estados, la política pública y la seguridad nacional.

Parecería ser que el punto de inflexión es a partir del 2016, momento en el cual la UE comienza a incorporar nuevas demandas en los acuerdos, que en su mayoría aún no han podido firmarse. Lo cierto es que a medida que empieza a haber mayor conciencia respecto de lo que se está entregando al firmar algunas cláusulas, más países comienzan a poner resistencia a los capítulos digitales en los Tratados de Libre Comercio (TLC). Este momento coincide con el lanzamiento de la Nueva Política Comercial de la UE²⁵ y la posterior aprobación (2016) y adopción (2018) de la Regulación General de Protección de Datos²⁶ (conocida como GDPR por sus siglas en inglés). Todas estas acciones van en línea con el Plan Estratégico 2016-2020 trazado por la Unión Europea en materia de negociación relativas al comercio²⁷ que incluyen como prioridad la economía digital y las nuevas demandas del mundo en materia de comercio de servicios.

La Conferencia Ministerial de Buenos Aires en el año 2017 dejó ver claramente este hecho, donde la mayoría de los países desarrollados querían impulsar una agenda de comercio electrónico, obteniendo mandato negociador para poder impulsar la agenda en la próxima Ministerial que iba a realizarse en Kazajistán en el año 2020. La resistencia por parte de los países subdesarrollados, sobre todo por parte del bloque de África, hizo que no fuera posible avanzar y obtener el mandato negociador. Algunos países parecen haber entendido lo que se está entregando, o al menos entender que se está dando acceso a una materia prima fundamental que aún no saben cómo procesar. Entregar a futuro y para siempre esa materia prima no parece ser la estrategia correcta. ¿Qué sucederá si algún día consiguen la capacidad de saber qué hacer con ella? Ya no tendrán nunca más acceso y a cambio se les ha dado la nada misma. No solo eso, sino que se está concediendo el derecho a negociar temas nuevos sin haber resuelto temas pendientes del pasado. En efecto, la Ronda de Doha sigue abierta y los países en vías de desarrollo siguen esperando una reparación histórica de las reglas de comercio de bienes y servicios que les permita avanzar hacia el desarrollo antes de incorporar temas nuevos en la agenda.

¿Qué motiva en el 2016 a la UE a cambiar su estrategia de comercio digital?

La Unión Europea, hasta ese momento, parecía una contempladora más de un proceso que la excedía. Pero en el año 2016 todo cambió. Las negociaciones de acuerdos de libre comercio que iniciaron, y que aún no han concluido, incorporan nuevas demandas en la búsqueda de avanzar en su industria digital que lleve a la UE a pensarse como actor de la economía del futuro.

La batalla por el 5G que está siendo disputada por China y EEUU parece dejar a Europa rezagada en brindar la infraestructura de la red. Sin embargo, la batalla por los servicios que va a permitir brindar

la nueva red puede poner al continente en un lugar de privilegio. La UE insertándose en las Cadenas Globales de Valor de manera inteligente implica subirse al extractivismo digital indiscriminado y colonialista que han llevado adelante las grandes empresas de tecnología con todos, incluso con la UE también. La acumulación de datos permite el desarrollo de nuevos servicios brindados a partir de empresas manufactureras. Parecería ser que la UE quiere asegurarse esa porción de mercado. La fabricación de heladeras o refrigeradores “inteligentes”, capaces de sugerirte que compres cosas o avisarte de ofertas especiales en tu barrio, anuncia nuevas oportunidades de beneficio e integración con otros productos y servicios (en comparación con una heladera o refrigerador “tonto” estándar). Todos esos servicios incorporados en la manufactura industrial sólo serán posibles si se tiene el almacenaje y procesamiento de datos.

En este sentido, este nuevo capitalismo digital que tiene como máxima aspiración la acumulación de datos, vino a transformar la economía en lo que se menciona en todos los foros internacionales, como la revolución 4.0²⁸. Es indudable que la UE, viendo cómo se le escapó la perdiz en el desarrollo embrionario de la misma, comenzó a cambiar su estrategia buscando insertarse en ese capitalismo a partir del desarrollo de cadenas de valor cibernético propiciadas por el extractivismo digital desde el sur hacia el norte global. Así, se puede ver como la Estrategia Europea de Datos²⁹ va en esa línea. Esta situación, propiciada por los fuertes lobbys³⁰ de las empresas tecnológicas norteamericanas en la región, habría hecho que la agenda cambiara radicalmente. Dichos lobbys no solo buscaron impulsar un modelo liberal en la economía digital en las relaciones comerciales, sino también hacia adentro de la UE tratando de evitar regulaciones que limiten su capacidad extractiva en el mercado europeo³¹.

Los tratados de comercio digital en negociación

En los últimos años, la agenda cambió. Nuevos temas se incorporaron a la negociación. El corazón de la agenda digital se hizo presente en los textos y, en la negociación, se establecieron como artículos básicos los que se refieren a la libre movilidad de datos. De alguna manera, se puede decir que Europa entendió el capitalismo digital, o, por lo menos, se hizo evidente que el extractivismo digital era la manera de obtener una masa crítica de datos que lleven a competir en el diseño de la economía del mañana.

Esto queda en evidencia al analizar las cláusulas presentes en las nuevas negociaciones actualmente en curso.

Cuadro 2: Acuerdos en negociación con cláusulas de comercio digital

Cláusulas	Túnez ³²	Chile ³³	Indonesia ³⁴	Australia ³⁵	Nueva Zelanda ³⁶	ESA ³⁷	OMC ³⁸
<u>Transferencia Transfronteriza de Datos</u>	NO	PARCIAL	SÍ	SÍ	SÍ	SÍ*	SÍ
<u>Prohibición de localización de datos</u>	NO	PARCIAL	SÍ	SÍ	SÍ	SÍ*	SÍ
<u>Prohibición de procesamiento de datos en el país</u>	NO	NO	SÍ	SÍ	SÍ	SÍ*	SÍ
<u>No divulgación del código fuente del software y algoritmos relacionados</u>	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Eliminación de impuestos aduaneros en productos digitales y/o transmisiones electrónicas</u>	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Autorización previa</u>	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO
<u>No discriminación contra productos digitales</u>	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Autenticación y firmas electrónicas</u>	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Protección online del consumidor</u>	NO	SÍ	PARCIAL	SÍ	SÍ	SÍ	SÍ
<u>Medidas contra comunicaciones electrónicas no solicitadas</u>	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
<u>Protección de datos personales y privacidad</u>	NO	NO	PARCIAL	PARCIAL	PARCIAL	PARCIAL	PARCIAL
<u>Responsabilidad de los intermediarios</u>	SÍ	PARCIAL	NO	NO	NO	NO	NO
<u>Compras públicas electrónicas</u>	NO	SÍ	SÍ	NO	NO	NO	NO
<u>Vigilancia</u>	SÍ	NO	NO	NO	NO	NO	NO
Año en que se comenzó a negociar	2015	2017	2016	2018	2018	2019	2019
Año de finalización de la negociación	Pausado 2019						

**Solo aplican a Mauritius, Seychelles y Zambia*

En el único acuerdo donde no se incluye el corazón del comercio digital es en Túnez, acuerdo que se encuentra frenado desde el 2019. Será cuestión de ver si, de reanudar las negociaciones, se decide incorporar estas problemáticas cláusulas.



4- LAS CONSECUENCIAS DE LA POLÍTICA DE COMERCIO DIGITAL DE LA UE PARA EL SUR GLOBAL

Lo que está en juego acá, es tener la libertad y soberanía de generar una estrategia de industrialización digital, versus una estrategia de colonialismo digital que someta a regiones enteras a ser meros consumidores de tecnología. Con la emergencia de un mundo global se espera que a través del Internet de las Cosas,

los electrodomésticos que utilizamos todos los días puedan generar datos y estos sean analizados, generando nuevos servicios. Los autos inteligentes, por ejemplo, no solo nos desplazan, sino que nos sugieren hacerle el service al vehículo, nos indican dónde podemos realizarlo cercano a nuestro domicilio, y nos avisan si algo está fallando. Si todos esos datos viajan y se almacenan en la Unión Europea, es allí donde se generarán nuevos puestos de trabajo más productivos de venta y comercialización de nuevos productos publicitarios y predictivos.

Ahora bien, ¿qué consigue la UE de aprobarse estos acuerdos? La principal ventaja es la capacidad de poder procesar datos y desarrollar esos nuevos servicios de puertas adentro del territorio que signifiquen nuevas exportaciones de la UE hacia los países periféricos. Difícilmente a esta altura la UE puede superar a gigantes como Google en el procesamiento de datos y en el desarrollo de inteligencia artificial, pero sí puede soñar con conseguir que las empresas se instalen en su territorio para almacenar, procesar y entregar datos que describen comportamiento y puedan ser utilizadas para venderse a otras empresas, generando servicios digitales nuevos.

A su vez, y este punto no es menor, con la llegada de los autos autónomos al mundo, las automotrices europeas podrían controlar los datos que se generan y mantener bajo su control estos servicios súper productivos de control de vehículos a través del “cerebro” y los sensores incorporados a los autos.

Toda una industria del procesamiento de datos se está gestando, tanto en recursos humanos, en logística, en servicios médicos, de entretenimiento, educación, transporte urbano inteligente, por mencionar algunos. Quedarse con los datos es permitir que las empresas locales europeas crezcan a expensas de un sur global cada vez más sometido, con unos términos de intercambio que se siguen debilitando, vendiendo materias primas a cambio del consumo tecnológico de la cotidianeidad.

Estos datos son llevados, en definitiva, de manera extractivista, sin dejar ingresos de ningún tipo, y sin poder siquiera cobrar aranceles por los servicios digitales importados. Un resultado perverso para la mayoría de la población global.

El posicionamiento Europeo en esta materia en los TLC (Tratados de Libre Comercio), juega a su favor vis a vis los países menos desarrollados. Pero, a escala global en la OMC, la agenda europea juega a favor de las grandes corporaciones norteamericanas unidas en GAFAM (Google, Apple, Facebook, Amazon y Microsoft) y en contra de China. De aprobarse la reglamentación de forma multi o plurilateral en la OMC, esta tendrá un carácter mucho más abarcativo, perdiendo Europa capacidad de extraer datos del sur global, teniendo que competir contra empresas norteamericanas. Es indudable que la capacidad de EEUU de absorber datos es infinitamente superior a la europea.

Vigilancia en la red, protección a los consumidores, autorizaciones para operar, licitaciones públicas. Todas medidas que buscan dar acceso a mercados a las empresas europeas en detrimento de las pequeñas empresas locales que puedan surgir en los países en vías de desarrollo. Europa busca expandir sus inversiones extractivistas hacia los países del sur, posicionando a sus empresas como líderes indiscutidos de un mercado que supo ser industrial y hoy se transforma a un capital cibernético.

Es indudable que Europa comprendió que, en el futuro, el capital cibernético subsumirá al capital industrial. Subirse a la agenda de libre comercio digital le permitirá a las empresas que tiene actualmente dar el salto tecnológico y transformarse en grandes empresas que desarrollen sus propios servicios digitales sin tener que tercerizar ese servicio a empresas norteamericanas. Si cada sector desarrollara su propia versión cibernética, no es lo mismo que esa versión sea dada desde afuera que de manera endógena desde dentro de la propia empresa. Europa parece estar preparando esta estrategia de acción para sus empresas, a fin de que salgan a competir en el mercado

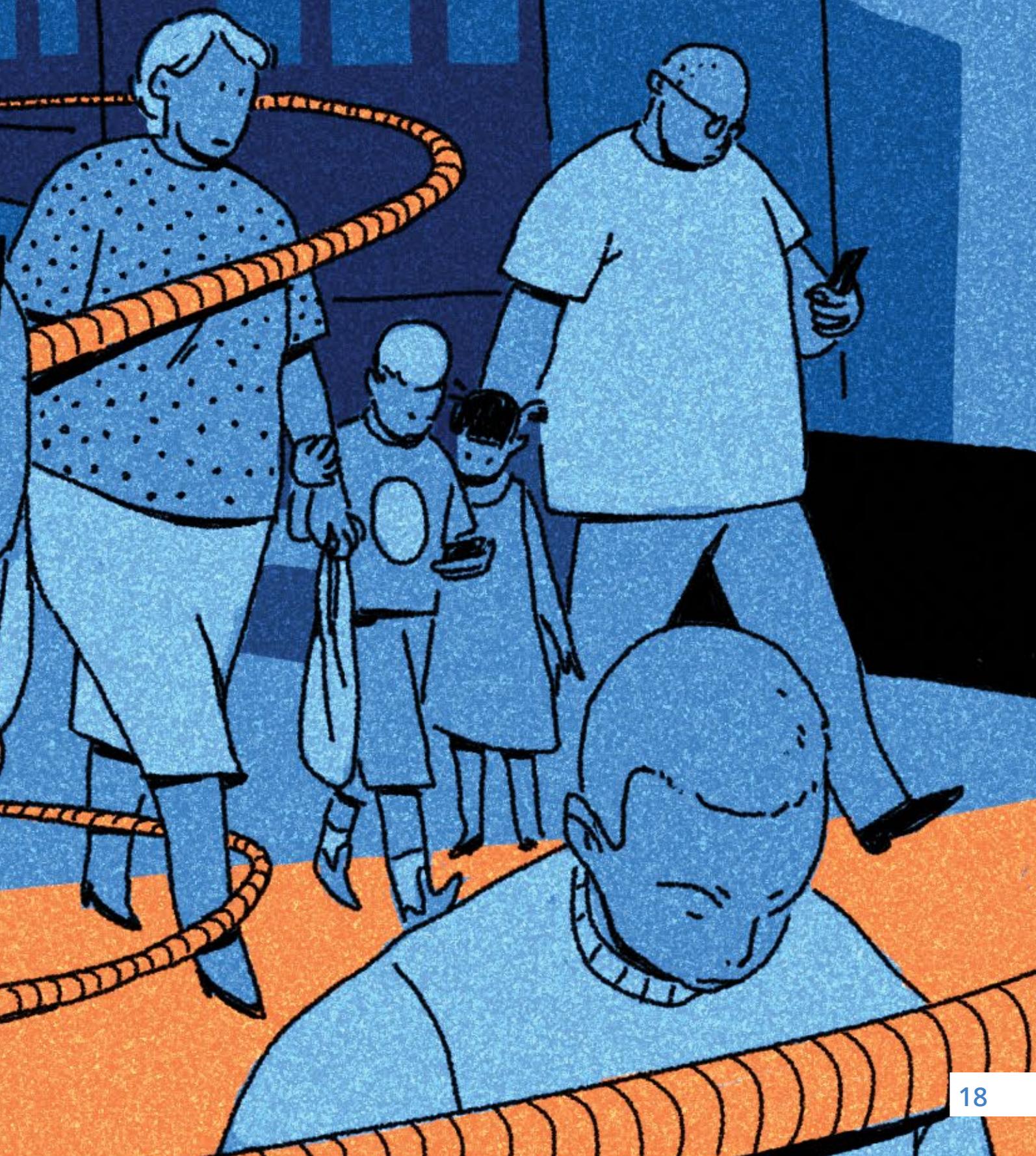
global, conquistan consumidores en mercados subdesarrollados y emergentes y conservando su capacidad exportadora. Un modelo de subsistencia basado en el extractivismo y en el subdesarrollo de la mayoría.

Esta agenda se impulsa en diversos foros y se utilizan excusas como promoción de las pequeñas y medianas empresas o igualdad de género. Existe un “lavado rosa³⁹” de la agenda de comercio electrónico, argumentando que las mujeres van a poder encontrar mejores empleos en la web, vendiendo productos y convirtiéndose en exportadoras a través de plataformas digitales⁴⁰. Lo cierto es que las mujeres a nivel global son las que menos acceso tienen a Internet⁴¹ y, cuando lo tienen, son las que hacen usos económicamente menos productivos de la herramienta⁴². Además, exportar implica no solamente tener Internet sino tener infraestructura y habilidades para sobrellevar trabas idiomáticas, informáticas, impositivas, de estándares, por mencionar algunas. El verdadero impacto es más subdesarrollo en la mayoría de los países del mundo para que unas pocas mujeres en países desarrollados puedan convertirse en exportadoras. Existe fuerte evidencia que indica que la agenda de comercio electrónico agrandará la brecha de género⁴³. No solo eso, sino que diversas organizaciones de mujeres ya se han manifestado en contra de la agenda de comercio digital⁴⁴.

Por otro lado, también se argumenta que las PYMES se benefician al abrirse mercados internacionales bastos que les permitan localizar productos. Con las reglas de comercio internacional aquí propuestas es obvio ver quiénes serán los grandes jugadores en el comercio global, desplazando a las pequeñas y medianas empresas de países periféricos, teniendo que competir con la entrada indiscriminada de productos internacionales al mercado local.

En definitiva, la agenda le abre las puertas a poder insertarse en una economía cada vez más dinámica, pero lo hace a expensas de quitarle esa posibilidad a muchísimos países del sur global. De puertas adentro, beneficia a empresas transnacionales de tecnología y grandes empresas industriales locales que busquen la transformación digital. El pueblo sigue quedando rezagado, sin posibilidad de tener una soberanía digital, dependiente del consumo tecnológico de productos producidos con una lógica extractivista y el objetivo claro de maximizar ganancias por sobre la sostenibilidad de la vida.

4- CONCLUSIONES



Durante años, Google, Apple, Facebook, Amazon y Microsoft (GAFAM) han intentado impulsar esta agenda en los acuerdos de libre comercio y otros espacios multilaterales de reglas comerciales. El éxito parcial que han tenido hasta ahora da cuenta de que todo el sistema de comercio mundial esta sistemáticamente alineado en contra de los intereses de los países menos desarrollados y, a medida que se les exige negociar temas nuevos, los viejos temas comerciales de agenda -como los subsidios agrícolas- siguen estando ahí, a la espera de una resolución favorable para aquellos países exportadores de materias primas.

Al principio de la década del 2000, no se alcanzaba a ver resistencia respecto de las negociaciones comerciales de la economía digital, pero a medida que el tiempo pasa, cada vez más países están tomando conciencia de la importancia de reconocer el valor de los datos como materia prima. La comprensión sobre su valor económico lleva a que, poco a poco, existan mayores resistencias a negociar acuerdo de comercio electrónico. No obstante esto, los esfuerzos por disfrazar esta agenda son realmente desconcertantes. Argumentos como “si no negociamos se va a acentuar la desigualdad”, “la economía digital es el futuro y necesitamos urgentemente reglas para ella”, y “favorece a las PYMES y a las mujeres, no les quitamos la oportunidad”⁴⁵, resuenan en los pasillos de la Organización Mundial de Comercio (OMC), y diversos espacios donde se promociona este tipo de acuerdos, empujando a los países a negociar una agenda que nada tiene que ver con lograr esos objetivos sino todo lo contrario: se quieren reglas que no permitan poner reglas. Un liberalismo digital a medida de las grandes potencias.

La cumbre Ministerial de la OMC en Kazajistán 2020 se canceló a causa de la pandemia del Covid-19, pero no por eso cesaron las negociaciones y se espera que dentro de muy poco tiempo se pueda cerrar el acuerdo de economía digital de los “Buenos amigos del comercio electrónico para el desarrollo”⁴⁶, como se autodenomina el grupo de países que está actualmente negociando la agenda de manera plurilateral. El 2021 nos recibe con una OMC que tiene una nueva Directora General, Ngozi Okonjo-Iweal⁴⁷. Por primera vez una mujer y africana preside la institución. Aunque todavía no está clara su postura, ha estado facilitando las conversaciones en torno al acuerdo plurilateral de comercio electrónico, aunque no tenga mandato para ello. No obstante, su nombramiento es esencial para que la agenda avance, dado su papel de facilitadora de los debates y de promotora de nuevos temas. El grupo de Amigos del Comercio Electrónico espera avanzar en el camino hacia la próxima Conferencia Ministerial de noviembre de 2021

La Unión Europea enfrenta el desafío de pelear una batalla que ya ha perdido: la supremacía digital hoy se debate entre dos países, EEUU y China. El plan es, pues, comenzar con una estrategia colonialista, yendo a la caza de datos del sur global, a fin de lograr posicionar a sus empresas en las nuevas cadenas globales de valor cibernéticas. Las empresas industriales tradicionales están evolucionando hacia la producción de servicios agregados a través de canales digitales, y las opciones son producirlos hacia dentro de las empresas europeas o tercerizar estos servicios a través de empresas tecnológicas. Abrir mercados y posicionar a las empresas europeas en otros países facilitaría el extractivismo digital y la capacidad cibernética de las empresas europeas. Sumado a eso, los lobbys de las empresas norteamericanas en la UE han llegado a niveles desmesurados, con reuniones constantes tratando de convencer a los negociadores europeos de firmar la agenda de comercio electrónico⁴⁸ diseñada por ellos mismos.

Pero, sobre todo, Europa no solo juega un juego económico, sino también político en la batalla entre China y EEUU. El debate ha impactado en empresas como Huawei, que han querido penetrar el mercado europeo ofreciendo dispositivos para 5G, y algunos países europeos le han cerrado las puertas a las inversiones, producto, sobre todo, de las presiones del gobierno norteamericano⁴⁹. Parece que Europa quiere ponerse del lado de la potencia reinante frente a la emergente en esta batalla por la supremacía. En cambio, el gigante asiático se ha centrado en consolidarse como líder indiscutible en Asia, principal inversor en África y fuerte influencia en América Latina, desplazando poco a poco a las potencias atlánticas y privándolas de aliados.

Esta estrategia tiene su correlato en acuerdos comerciales, donde el RCEP (Regional Comprehensive Economic Partnership)⁵⁰ ya se encuentra concluido, constituyendo un bloque comercial sin precedentes en la región oriental. La guerra comercial entre ambas potencias en América Latina ya está declarada. El temor de EE.UU. a la creciente influencia de China en “su patio trasero” puede verse en el reciente cabildeo de EE.UU. en la elección del presidente del Banco Interamericano de Desarrollo para limitar las acciones de China en la región⁵¹. El temor de EE.UU. a la estrategia de las empresas chinas en la región hizo que estuviera dispuesto a romper un pacto histórico con la región (ya que el acuerdo era que el presidente del BID debía ser de América Latina) para nombrar a un ciudadano estadounidense, Claver Carone, con el fin de restringir la expansión de las inversiones asiáticas en la región.

Europa apuesta a continuar con el modelo que le funcionó hasta la fecha: EEUU de aliado indiscutido para fortalecer una región atlántica que haga negocios inteligentemente con Asia. El intento fallido de firmar y aprobar el TTIP (Transatlantic Trade and Investment Partnership)⁵² iba en esa dirección. La presencia de los movimientos sociales como principales motores de resistencia y activismo fue clave para no lograr consolidar una alianza que pudo haber llevado a la hegemonía del bloque en detrimento de los más débiles, costando soberanía y la democracia de los pueblos.

Lo cierto es que las reglas de la economía digital ya están escritas⁵³ y no favorecen a las personas. No buscan fortalecer a los gobiernos y las democracias sino que fueron escritas para, por y en beneficio de las grandes empresas de tecnología, dándoles mercado, recursos gratuitos, capacidad monopólica ilimitada y ninguna responsabilidad social ni impositiva. Frente a este robo de recursos, a este extractivismo digital, y a esta práctica monopólica, solo queda conservar la libertad de los Estados para regular. Por nuestras economías, pero sobre todo también, por nuestra soberanía, nuestra cultura y nuestra democracia. No hay posibilidad de crear un mundo más justo si los bolsillos de los más ricos se siguen llenando a costa de la producción de los más pobres a través del extractivismo de materias primas. No hay paz posible sin justicia social.

Esta postura lejos está de ser anti tecnológica. La tecnología siempre fue aliada de la humanidad. La tecnología nos atraviesa y nos constituye como sociedades. Simplemente se trata de creer que es posible un desarrollo tecnológico con otra lógica, que ponga al ser humano, a la distribución de la riqueza, y al beneficio de los pueblos en el centro de la diagramación de los sistemas que gobernarán nuestras vidas de cara al futuro.

Lamentablemente, no firmar estos acuerdos no es garantía de que esa economía vaya a desarrollarse, pero definitivamente deja la puerta abierta para que aquel país que se atreva a pensar otro futuro posible, tenga la capacidad de construirlo. Firmarlos es condenarnos. No firmarlos es el comienzo de una larga y difícil historia posible de industrialización y soberanía digital. “No nos tiren la escalera al desarrollo digital” podría bien ser la nueva bandera que se enarbole, permitiéndole a los países en vías de desarrollo tener una vía por la que subir esos peldaños que necesitan para eliminar bolsones de pobreza y desigualdad.

La estrategia europea puede evaluarse como un intento de insertarse en un mundo que tiene muchas ganancias por explotar, pero es una carta peligrosa de jugar, condenando a otros países al subdesarrollo y permitiendo, a su vez, que otras empresas moldeen su democracia y su economía sin capacidad de regulación.

En un mundo incierto, donde la acumulación desmedida de capital no cesa y en un momento donde ha cambiado el poder geopolítico, conservar la capacidad regulatoria para proteger a sus ciudadanos, cooperar en la expansión de nuevos polos digitales competitivos y promover la eliminación de guaridas fiscales, así como el pago de impuestos de puertas adentro de estos verdaderos gigantes tecnológicos, es el camino más sustentable, más democrático y con mayor equidad e inclusión para todos y todas.

ANEXO: LAS CLÁUSULAS DE COMERCIO DIGITAL Y SUS EFECTOS

TRANSFERENCIA TRANSFRONTERIZA DE DATOS

¿Qué dice?

Las Partes se comprometen a garantizar los flujos de datos transfronterizos para facilitar el comercio en la economía digital⁵⁴.

¿Que implica?

Extractivismo digital

Esto significa que los datos –la materia prima de la inteligencia artificial– y otras tecnologías de la nueva revolución industrial pueden cruzar las fronteras y el Estado pierde el acceso a ellos. Implica que cualquier empresa que comience a tener operaciones en el territorio con el que firmó el acuerdo, puede extraer datos de los consumidores y ciudadanos locales y llevarlos a otro territorio sin ningún tipo de restricción. Esto es crucial comprenderlo: una vez que los datos atraviesan la frontera, no se puede exigir acceso o repatriación porque el país pierde jurisdicción sobre los mismos. Es el equivalente de cualquier bien físico que conozcamos. Supongamos una obra de arte o un mineral precioso: una vez que atraviesa la frontera, al país le va resultar muy difícil conseguir que ese bien regrese al territorio, si es que alguna vez puede hacerlo.

Ejemplo

Una de las preocupaciones centrales en cuanto a aprobar el flujo transfronterizo (o transferencia) de los datos, es la afectación de la privacidad de los ciudadanos, principalmente en cuanto a los datos sensibles, como pueden ser los de la salud. En ese sentido, y teniendo en cuenta la realidad de venta y compra de bancos de datos en la industria de la salud, países como Australia, entre otros, tienen leyes estrictas de privacidad. En el caso del gobierno australiano, la ley de privacidad australiana es más difícil de hacer cumplir si el proveedor de los servidores de almacenamiento de datos tiene su sede en el extranjero. Es por este motivo que el sistema de registros de salud electrónicos de Australia tiene como requisito que los datos permanezcan y se procesen en Australia. Si se aprobara una transferencia transfronteriza de datos indiscriminada, Australia no podría establecer la protección necesaria para la privacidad de los datos de salud de sus ciudadanos. Esto se debe, además, a las preocupaciones que existen en cómo puede utilizarse el big data, sobre todo en ese ámbito, que es una de las industrias que más factura (medicina prepaga, clínicas privadas, industria farmacéutica, laboratorios)⁵⁵. La Unión Europea cuenta con una ley que protege la privacidad de los datos de sus ciudadanos conocida como GDPR⁵⁶. Cabe aquí la pregunta de qué pasaría si los datos son llevados a otras locaciones donde no existen leyes que regulen estas cuestiones. La ley contempla este hecho y protege a los ciudadanos europeos, dándole a la ley jurisdicción extraterritorial. La UE afirma estar desarrollando sistemas para asegurar que la ley de protección de datos europea pueda ser aplicada en cualquier lugar del mundo⁵⁷. En todo caso, se necesitan generar mejores sistemas de auditoría y control a nivel global para verificar que se respete la privacidad de los ciudadanos en todo el mundo. No obstante, es difícil exigir estas mismas cosas a los países en vías de desarrollo,

ya que no cuentan con los mismos recursos para poder desarrollar dichos sistemas, a la vez que la debilidad institucional hace que muchas veces no cuenten con una buena ley que proteja los datos personales de sus ciudadanos.

En términos de desarrollo económico, esta minería de datos representa una materia prima vital para el desarrollo de la inteligencia artificial que, bajo esta norma, se va del territorio y jamás vuelve a ingresar. También es información relevante a la hora de diseñar una política pública. Pensemos por un momento cuanto valdrían los datos de UBER para poder desarrollar una política de planeamiento urbano en el sistema de transporte, o los datos de Google Classroom durante la pandemia del Covid-19 para el ministerio de educación de cualquier país. Poder exigir acceso a los datos es vital para el diseño de futuras políticas públicas efectivas.

PROHIBICIÓN DE LOCALIZACIÓN DE DATOS Y PROCESAMIENTO

¿Qué dice?

Las corrientes transfronterizas de datos no se restringirán entre las Partes por:

- a. exigir la utilización de instalaciones informáticas o elementos de red en el territorio para su procesamiento, incluso imponiendo el uso de instalaciones informáticas o elementos de la red que están certificados o aprobados en el territorio de la Parte;
- b. requerir la localización de los datos en el territorio de la Parte para su almacenamiento o procesamiento;
- c. prohibir el almacenamiento o procesamiento en el territorio de la otra Parte;
- d. supeditar la transferencia transfronteriza de datos al uso de las instalaciones informáticas o elementos de la red en el territorio de la Parte o al ser localizados en el territorio del Partido⁵⁸.

¿Qué implica?

Eliminación de la escalera digital del desarrollo

Los datos como materia prima tienen diversas instancias en su cadena de valor. El movimiento del dato que lo hace atravesar la frontera conforma la exportación de esa materia prima. Pero la cadena de valor también tiene como componentes fundamentales el procesamiento y alojamiento del dato. Estos pueden ocurrir independientemente de la exportación del mismo. Si podemos resumir brevemente esta cláusula, diríamos que es colonialismo digital y dependencia económica. Un país podría poner en su sistema de compras públicas, al contratar proveedores digitales, cláusulas contractuales que pidan que esos datos se queden en el país y se le dé acceso al Estado a fin de diseñar políticas públicas o, en un futuro, sus propios sistemas que puedan reemplazar al proveedor y lograr independencia económica y contribuir a la industrialización digital. Por su parte, bien podría sancionar una ley que contenga requisitos mínimos para cualquier empresa que invierta en el territorio. Con esta cláusula en los acuerdos de libre comercio quedaría limitada dicha capacidad. Esto es utilizado actualmente por algunos países y fuertemente resistido desde los grupos de lobby hegemónicos⁵⁹. Las corporaciones argumentan que los requisitos de localización permiten abusos en el acceso de los Estados a los datos. A su vez, se argumenta que si bien protegen a la industria nacional en el corto plazo, al no generar competencia con el exterior, termina yendo en detrimento de la economía. En otras palabras, la localización de datos en el territorio no favorece los intereses de las empresas transnacionales y les hace más difícil competir contra las empresas locales.

Lo cierto es que la localización de datos es un asunto estratégico en la economía actual y futura, ya que tener servidores de datos cercanos permite varias cosas. Por ejemplo:

- Tener sistemas de información más veloces y efectivos, ya que de lo contrario se produce una triangulación. Un ciudadano utiliza un servicio y solicita una búsqueda en la web, ese pedido debe “viajar” hasta el servidor donde se encuentran los datos, debe ser procesada la solicitud, y debe volver con el resultado. Esto se demora unas milésimas de segundos y es casi imperceptible para la población, pero, con la llegada del 5G, este será de vital trascendencia⁶⁰. En efecto, para manejar un auto inteligente o realizar una cirugía remota es necesario que esa demora no exista porque puede costar vidas humanas.
- Que los datos queden bajo la jurisdicción del país que los produce permite también eventualmente pedir acceso a los mismos por causas de salud o seguridad nacional entre otros. Otorga soberanía sobre los mismos, permitiendo que este insumo estratégico quede dentro de los confines de un país y de aquellos que los produjeron. Hoy en día, si un gobierno necesita datos de, por ejemplo, Google, debe pedir permiso al Departamento de Estado de los EEUU para que a su vez este organismo los solicite a Google y finalmente sean compartidos⁶¹.
- Genera subsistemas económicos de alta tecnología, ya que un centro de almacenamiento y procesamiento de datos requiere de personal especializado en el ensamblaje y mantenimiento del mismo, producción de hardware y software para operarlo, redes de fibra óptica que lleguen hasta el mismo, y, en muchos casos, hasta energías renovables para alimentarlos. Muchas empresas comenzaron a invertir en sistemas energéticos autónomos para sus data centers debido al riesgo que implica la pérdida de energía como resultado de una falla en el sistema energético nacional, el ahorro de costos que puede traer, además de minimizar el impacto ambiental⁶².
- El procesamiento, por otro lado, generalmente se realiza en el lugar donde se almacenan los datos para evitar una doble triangulación que hace más lenta la entrega final del producto. Este punto es clave también, porque ahí es donde se genera la mayor ganancia de la economía capitalista cibernética. Ese procesamiento no es ni más ni menos que los sistemas algorítmicos de procesamiento de datos en tiempo real y donde hay mayor cantidad de trabajo humano de altísima productividad tecnológica. Un centro de procesamiento de datos requiere de ingenieros, programadores, matemáticos, y todo tipo de trabajadores altamente calificados⁶³.

Ejemplo

Uno de los motivos centrales para mantener la localización del almacenamiento y procesamiento de los datos, es la seguridad. Sobre todo en cuestiones que podrían afectar la seguridad nacional de un país. Este es el principal motivo de los Estados Unidos que tienen como requisito que todos proveedores de servicios de computación en la nube que almacenen datos del Departamento de Defensa deben estar dentro de sus fronteras⁶⁴. Por otro lado, otro motivo para mantener la localización es tener la capacidad de hacer cumplir la legislación del país y evitar que las disputas legales se resuelvan en cortes internacionales o extranjeras. En el caso de Nueva Zelanda, su gobierno requiere que los registros de impuestos que estén almacenados “en la nube”, se almacenen en servidores ubicados en Nueva Zelanda y el no hacerlo es un delito punible con una multa. Si están habilitadas las copias de seguridad en la nube, siempre que los registros comerciales primarios se almacenen en Nueva Zelanda⁶⁵. De aprobarse esta normativa en el plano multilateral a través de la Organización Mundial de Comercio, podríamos ver, además, “Paraísos de datos”⁶⁶ emulando a los ya conocidos

paraísos fiscales: lugares donde las empresas transnacionales pueden alojar sus datos sin tener que respetar normativas de seguridad ni de protección de datos ni limitación al procesamiento de los mismos, para obtener el máximo de ganancia posible. Estos paraísos ya existen, pero de instalarse la normativa a nivel global, sería aún más difícil combatirlos para los Estados.

Asimismo, los ingresos registrados por el procesamiento y almacenamiento de datos vienen creciendo a nivel global⁶⁷. Los ingresos por tener almacenados datos en un país vienen creciendo a pasos agigantados, y de la ganancia total por dicho servicio, el 59.6% recibe EEUU, el 20% Europa occidental, el 10% Asia-Pacífico y el resto está repartido entre África, América latina y Europa oriental⁶⁸. Claramente el negocio de almacenar datos en nube pública se concentra en regiones determinadas con una fuerte estrategia de extractivismo digital. Sin embargo, el incremento del ingreso no solo se registra a nivel estatal, sino también dentro de las propias empresas. Por ejemplo, en la actualidad en el caso de la empresa Visa, el 38% de las ganancias provienen del procesamiento de datos⁶⁹.

NO DIVULGACIÓN DEL CÓDIGO FUENTE DE SOFTWARE Y ALGORITMOS RELACIONADOS

¿Qué dice?

Ninguna de las Partes podrá exigir la transferencia del código fuente de los programas informáticos propiedad de una persona jurídica o física de la otra Parte, ni el acceso a los mismos.⁷⁰

¿Qué implica?

Desigualdad, pobreza, exclusión y competencia desleal.

Para comprender de manera amplia esta cláusula en los acuerdos de libre comercio hay varios conceptos que necesitan ser explicados previamente. Por un lado, ¿qué es un algoritmo? En la economía digital todo se maneja con ellos y es lo que realmente procesa la enorme cantidad de datos que generamos a diario. Los algoritmos son instrucciones, ecuaciones matemáticas, que procesan información y devuelven un resultado, sea una maximización u optimización (predicción estadística), un ordenamiento, una decisión o un menú de opciones. Cuando hacemos una búsqueda en Internet, un algoritmo decide qué resultados veremos primero; cuando ingresamos a Netflix, un algoritmo decide qué películas mostrarnos; un algoritmo procesa imágenes médicas e indica cuál es la probabilidad de que determinada mancha sea un tumor; un algoritmo asigna pedidos a repartidores que trabajan en plataformas cuando van por las calles entregando pedidos.

Esto es lo que se conoce como Machine Learning y Deep Learning, dos tipos de tecnologías dentro del campo de la Inteligencia Artificial, y ya está ampliamente documentado que tiene algunos inconvenientes difíciles de solucionar. El concepto de sesgo algorítmico acá es clave. Los algoritmos tienen sesgos de fabricación muy importantes que, si bien pueden ser minimizados, es poco probable que sean completamente eliminados. Para empezar, los algoritmos se alimentan de datos, pero esos datos son categorizados y separados de manera arbitraria. Desde la categoría sexual binaria hasta la elección de posibilidades de frutas y verduras, las categorías que se eligen para ingresar datos pueden ser sesgadas y dejar grupos enteros de datos sin ser registrados y, por ende, no tenidos en cuenta por un algoritmo. A su vez, los datos se cargan con historiales de violencia y discriminación. Por ejemplo, se ha estudiado que las mujeres choferes de UBER en EEUU ganan un 7%⁷¹ menos

que sus colegas hombres, no debido a que manejen peor ni a que sean peores anfitrionas a la hora de llevar un pasajero, sino a que la población tiende a calificarlas más negativamente que a los hombres por aspectos culturales. Finalmente, existe un sesgo de programación que es, seguramente, el más importante. La decisión de qué es importante y qué no para un algoritmo es, en definitiva, una decisión humana. Cathy O'Neil tiene un ejemplo muy clarificador⁷². Ella argumenta que tiene un algoritmo en su cabeza que decide todas las noches qué cocinar para la cena. Las variables que posee es valoración nutricional, elementos que tiene en la heladera, ganas y tiempo de cocinar, lo que comió al mediodía, gustos de la familia, etc. Su cabeza procesa eso y decide qué cocinar ese día específico. ¿Qué pasaría si su hijo tomara el control del algoritmo? Seguramente la nutrición pasaría a un segundo plano y los gustos serían predominantes, teniendo como resultado unas papas fritas por sobre un pescado. Los sesgos son muchos y tienen impactos enormes sobre las sociedades. Si le sumamos a eso el factor de que la mayoría de los algoritmos que utilizamos a diario son programados en países desarrollados por hombres blancos, de un nivel socioeconómico y educativo determinado, corremos riesgo de que las minorías, disidencias y mujeres jamás sean tenidas en cuenta. En efecto, solamente existen a nivel mundial un 22% de mujeres programadoras. En USA, la mayor economía en la industria, el 67.7% de los programadores son blancos, 19.5% son asiáticos y menos del 13% son personas negras y de otras etnias. Los latinos ni siquiera son contabilizados en las estadísticas⁷³.

Ahora bien, ¿por qué es importante todo esto? Porque el artículo claramente prohíbe que se publique el algoritmo y el código fuente. Cabe aclarar que a los efectos estrictamente técnicos, el algoritmo es la orden dada y el código fuente es la instrucción o el cómo se piensa desarrollar esa orden. Yendo a un ejemplo jurídico, el algoritmo es la ley, el código fuente sería la reglamentación.

En algunos países, como es el caso de Argentina, el software (código fuente y el ejecutable) está protegido bajo la Ley de Propiedad Intelectual, en el marco del derecho de autor. En estos casos, a pesar de existir esa protección para sancionar copias ilegales, por ejemplo, no se impide el acceso a leer el código. Esa prohibición podría darse si el código o algoritmo estuviera protegido por el secreto industrial, como hacen algunas empresas. Por otro lado, en otros países, como es el caso de Estados Unidos o Canadá, el software está protegido bajo el sistema de patentes, que son títulos que reconocen el derecho de explotar en exclusiva durante 20 años funcionalidades, algoritmos, representaciones y otras acciones que se pueden llevar a cabo con una computadora. En el caso de las patentes, para otorgar esa exclusividad, el código también se hace público y nadie más puede utilizar ese código por el periodo que dure la patente.

Si no tengo acceso, no puedo auditarlo para saber qué problemas está teniendo en caso de que algo malo ocurra. La cláusula suele incluir excepciones como en el caso de defensa y seguridad nacional o si hay sospechas de que el algoritmo es contrario a las leyes de competencia del país. Lo cierto es que es difícil armar un caso que demuestre la necesidad de auditar el algoritmo y que las excepciones no toman en cuenta problemas en la población en general, como el caso de discriminación a trabajadores o en sistemas de reconocimiento facial, por mencionar algunos.

Por otro lado, también cabe aclarar que aun cuando se pueda auditar el código fuente, casi nunca es simple encontrar cuál es el error o identificar el problema que ha surgido. Los algoritmos, en muchos casos a través de Machine Learning, se auto-escriben y terminan siendo ilegibles para los propios programadores. También hay que destacar que en promedio, los programas de código abierto⁷⁴ son más fiables que los de código cerrado⁷⁵, por lo cual estos traen más beneficios sociales por los motivos antes descritos.

En conclusión, es un problema muy complejo de resolver que la humanidad recién está empezando a enfrentar y que puede tener impactos múltiples en nuestras sociedades generando a futuro discriminación, problemas ambientales, ataques a la democracia y desestabilización económica, entre otros. No parece ser, a simple vista, una buena medida limitar la capacidad estatal ante un problema que recién comenzamos a conocer y que aún no sabemos cómo solucionar. La no divulgación de los algoritmos ha sido problemática hace ya muchos años. Así, aun en los acuerdo de libre comercio, los países han comenzado a poner más y más excepciones⁷⁶.

Ejemplo

El acceso al código fuente puede ser solicitado para casos judiciales por ejemplo para casos de violación de propiedad intelectual de un software, de precisión en los diagnósticos y resultados (por ejemplo, en el caso de un presunto conductor ebrio que quisiera conocer la precisión del sistema de un alcoholímetro). También para saber si el sistema genera o reproduce discriminación en determinadas poblaciones, se puede necesitar acceder al código para estudiarlo y así disminuir las vulnerabilidades al hackeo (por ejemplo en sistemas de voto electrónico o utilizados en áreas sensibles como puede ser el ámbito de la salud, la seguridad y la administración pública, la infraestructura crítica -como centrales de energía nuclear-, entre otros). Uno de los motivos que pueden tener los gobiernos para requerir acceso al código fuente puede ser para comprobar que se esté cumpliendo con alguna regulación en particular. Un ejemplo de esto es el escándalo de las emisiones de Volkswagen, cuando la empresa de automóviles utilizó el software para superar la prueba de emisiones aunque, en realidad, estaba contaminando hasta 40 veces más que el límite legal al conducir.⁷⁷

ELIMINACIÓN DE IMPUESTOS ADUANEROS EN PRODUCTOS DIGITALES Y/O TRANSMISIONES ELECTRÓNICAS

¿Qué dice?

Las Partes acuerdan que las transmisiones electrónicas se considerarán como suministro de servicios, y ninguna de las Partes podrá imponer derechos aduaneros a las transmisiones electrónicas⁷⁸.

¿Qué implica?

El vaciamiento y la desfinanciación del Estado son un hecho en esta cláusula.

Si algo vimos durante la pandemia del Covid-19 es que muchas de las cosas que pensamos que jamás iban a ser posibles de digitalizar, lo son. Educación, teletrabajo y telemedicina fueron los grandes cambios, pero otros que venían ganando mercado tímidamente, se aceleraron, como el caso de reuniones y seminarios online, por mencionar algunos. Lo cierto es que a medida que avance la tecnología, cada vez más proporción de la economía va a poder ser distribuida a través de Internet. De hecho, el proyecto del 5G planea crear ciudades, fábricas y hogares inteligentes, con maquinaria y electrodomésticos que se manejan de manera remota desde otros países⁷⁹. Ciudades donde los autobuses no posean choferes y el conductor esté probablemente en un centro de datos en algún territorio alejado y sea un algoritmo. Las impresoras 3D permiten comercializar diseños a través de la web que pueden ser impresos directamente en el país que adquiere el diseño. Esto abre un mundo nuevo en las exportaciones de servicios digitales, desplazando a las exportaciones manufactureras.

En este sentido, prohibir las tasas aduaneras a las transmisiones electrónicas implica no poder cobrar impuestos en frontera por ninguno de estos servicios provistos desde el exterior. Es una desfinanciación del Estado a futuro.

Si bien es cierto que la cláusula no impide cobrar impuestos internos (como impuesto al valor agregado, por ejemplo), sí impide cobrar impuestos aduaneros, lo que deja ver que la intención no es otorgarle menores precios a los consumidores, sino que el objetivo es bien distinto. Cuando los impuestos son aduaneros, es el Estado el que los cobra directamente al ingresar al territorio y hacen que los productos nacionales tengan un trato diferenciado de manera indirecta, puesto que no deben pagarlo. Abarata el precio de las mercancías de producción nacional contra las que se producen fuera del territorio. En cambio, los impuestos internos los cobran las empresas directamente al usuario y es esa misma empresa la que es encargada de girar ese dinero al Estado. Esto tiene varios efectos positivos para las empresas transnacionales. En primer lugar, sólo aquella empresa que posea infraestructura digital lo suficientemente grande para diferenciar los impuestos de cada país en el que opera, podrá ganar mercado. A los competidores pequeños se les hará difícil sostener esa estructura y serán más propensos a cometer errores y por ende, perder la competencia. En segundo lugar les da posesión de divisas extra que pueden demorar en el pago, pudiendo producir intereses extra con el manejo de esos fondos. En tercer y último lugar, las normas de trato nacional hacen que de cobrarles un impuesto interno a las multinacionales, ese impuesto deba ser aplicado también a sus competidores locales. Las economías de escala juegan un papel fundamental ahí donde es mucho más probable que las empresas nacionales no puedan competir a los precios baratos que suelen tener las multinacionales y terminen perdiendo mercado.

En una economía cada vez más digital y globalizada, no poder cobrar impuestos aduaneros a las transmisiones electrónicas es quitarle al Estado su principal fuente de financiación y su capacidad de industrialización digital nacional y soberana, perdiendo empresas tecnológicas nacionales a manos de la competencia internacional.

Esta norma, si bien se está negociando en Tratados de Libre Comercio, ya existe en la OMC hace años a través de la Moratoria de los Derechos de Aduana en las Transmisiones Electrónicas (MDATE). La misma se acordó de forma multilateral en el año 1998, mucho antes de tener dimensión de lo que iba a ser la revolución digital, de que existieran los teléfonos inteligentes y de que las redes sociales modificaran la forma en la que nos comunicamos e informamos.

La MDATE básicamente replica la cláusula de no pagos de impuestos a las transmisiones electrónicas de los acuerdos de libre comercio pero en el plano multilateral, impidiendo desde el año 1998 que los países en vías de desarrollo y subdesarrollados, importadores netos de servicios digitales, puedan cobrar impuestos aduaneros por los mismos. Esta moratoria se renueva año a año desde ese momento y jamás se ha podido revertir, generando una verdadera pérdida fiscal para el sur global.

La inclusión de esa cláusula en los acuerdos de libre comercio tiene como fin lograr que si alguna vez no se renueva la moratoria, se siga sosteniendo el compromiso a través de la diversidad de TLCs que existen.

Ejemplo

La liberalización digital probablemente facilitará más importaciones de productos y servicios con alto contenido digital en los países en desarrollo, en lugar de exportaciones desde ellos. Los proponentes disfrazan sus propuestas alegando que son necesarias para “dar rienda suelta al desarrollo a través del poder de las MIPyMEs (Micro, Pequeñas y Medianas Empresas) que utilizan el comercio electrónico”. Pero para comerciar, los países deben generar e incrementar el valor capturado de la producción. Si el comercio digital se expande sin mejorar primero las capacidades productivas y la infraestructura digital (como las mejoras en la infraestructura física y la interconectividad y la adopción de normas aplicables para la privacidad, la protección de datos y los derechos de datos económicos), los países en desarrollo simplemente abrirán sus economías aún más a las importaciones extranjeras⁸⁰.

Global Financial Integrity identificó a empresas transnacionales que, en 2014, drenaron entre 620 y 970 mil millones de dólares de los países en desarrollo, principalmente mediante dudosas maniobras comerciales⁸¹. Un ejemplo es Uber que utiliza subsidiarias con sede en Irlanda y los Países Bajos para registrar la gran mayoría de sus ganancias, acumuladas a su propiedad intelectual, en el paraíso fiscal de las Bermudas, dejando países (desde Kenia hasta los Estados Unidos) donde se generan las ganancias, sin derechos tributarios apropiados⁸². La OMC los protege para no pagar aranceles, y además utilizan subsidiarias en paraísos fiscales para evadir impuestos locales.

En un documento elaborado por la UNCTAD se realizó un ejercicio de simulación que muestra que si esta moratoria se vuelve permanente, es decir, cero aranceles aduaneros a los productos y transmisiones electrónicas, habrá un aumento adicional de las importaciones de estos productos hacia los países en desarrollo, mientras que las importaciones de los países desarrollados no se verán afectadas. En muchos casos, no todas las importaciones en esta categoría son transmisiones electrónicas, por ejemplo, en el caso de los CD de música, o libros físicos, todavía hay algunas importaciones que no son transferencias electrónicas. A medida que aumenta la digitalización de productos y los consumidores eligen comprar un e-book o descargarse música a través de plataformas, más de estos productos se incluirán en la categoría de transferencia electrónica. El aumento de las importaciones de este tipo de productos, que actualmente se encuentran en esta categoría, será más alto en términos absolutos para China, seguido por India, Rusia y Brasil.⁸³

AUTORIZACIÓN PREVIA

¿Qué dice?

1. Las Partes se esforzarán por no exigir una autorización previa por el mero hecho de que el servicio se presta por medios electrónicos o adoptar o mantener cualquier otro requisito que tenga efecto equivalente.
2. El párrafo 1 no se aplica a los servicios de telecomunicaciones y financieros.
3. Para mayor certeza, nada impedirá a una Parte adoptar o mantener medidas incompatibles con el párrafo 1 para lograr un objetivo legítimo de política pública de conformidad con el derecho a regular, excepción general, las excepciones relativas a la seguridad, las excepciones cautelares.⁸⁴

¿Qué implica?

Incapacidad del Estado para controlar quienes operan en el mercado.

En los sectores de finanzas y telecomunicaciones es donde más se ven ejemplos de este tipo. Muchas veces los Estados exigen autorización previa para ingresar al mercado local. Esto permite regular la cantidad de competidores que va a haber y el tipo de servicio que van a brindar. Se hacen exigencias de requisitos mínimos y, en el caso de las telecomunicaciones, hasta se debe licitar espectro para poder empezar a ofrecer el servicio de telefonía móvil. Este principio promueve que no se pueda exigir autorización previa de este tipo para ningún servicio que sea brindado por medios electrónicos. Con la excepción de los dos sectores previamente mencionados, claro está.

Ejemplo

Esta situación genera varios inconvenientes. Por un lado, en muchos países empezaron a surgir aplicaciones como UBER o Airbnb que quieren ingresar a las ciudades y que ya son bien conocidos los problemas que generan⁸⁵ y cómo se las ha restringido en algunos lugares del mundo⁸⁶. De firmar estos acuerdos, dificultaría pedir autorización previa para ingresar a una ciudad, dejando a la aplicación la libertad de entrar al mercado que le plazca. Cabe señalar que acá se están comprometiendo todos los servicios entregados de forma digital presentes y futuros, con lo cual ante la emergencia de nuevas tecnologías desconocidas hasta el momento, el país quedaría limitado para detener la entrada de empresas que puedan afectar la economía nacional o proteger competidores frente a industrias nacientes.

El artículo dice que solamente se pueden hacer excepciones frente a restricciones para alcanzar objetivos de política pública *legítimos*. Como suele ocurrir en este tipo de acuerdos, no se expresa qué se considera legítimo y queda a interpretación de los jueces de tribunales en la OMC u otros tribunales internacionales que suelen fallar en favor de las empresas y en detrimento de los Estados.

NO DISCRIMINACIÓN CONTRA PRODUCTOS DIGITALES

¿Qué dice?

En sentido estricto, muy pocos o casi nulos acuerdos tienen cláusulas expresas que manifiesten la no discriminación de productos digitales. Sin embargo, esta está implícita en todo acuerdo a través de los principios de Acceso a los mercados y Trato nacional.

Un acuerdo de libre comercio, ya sea de carácter bilateral, plurilateral o las negociaciones realizadas a nivel multilateral en la OMC, siempre tiene incluidas estas cláusulas que básicamente determinan que no se puede hacer diferencia entre un producto y otro a la hora de fijar aranceles, subsidios, beneficios impositivos o cualquier otra medida que modifique las condiciones de comercio.

Al incluir los productos digitales en los acuerdos de libre comercio, se está incorporando el Trato nacional y el Acceso a los mercados a todos los productos digitales, a menos que estén expresamente escritos en las excepciones.

Así, un producto digital no puede ser tratado de una manera menos favorable que otros productos contenidos en el acuerdo ni de forma discriminada respecto al trato que reciben los productos de fabricación nacional. A su vez, no se le pueden restringir los mercados en los que se pueden ofrecer productos digitales o entregables a través de medios digitales.

¿Qué implica?

Esta regulación implica una pérdida de soberanía para tomar decisiones sobre cómo los Estados desean que de conforme el mercado de bienes y servicios, sobre todo los servicios públicos.

A medida que los servicios digitales avancen, más cantidad de servicios serán ofrecidos por esta vía. La educación, por ejemplo, era un servicio, sobre todo en el caso de la educación primaria y secundaria, que típicamente no era transable. Muchas veces los Estados protegían estos sectores por ser servicios públicos fundamentales y a fin de conservar soberanía sobre todo el proceso de producción del servicio educativo. Si a partir de la emergencia del Covid-19 la educación cambia y se empieza a brindar a través de plataformas digitales de forma permanente, ¿ese es un servicio educativo, uno digital, o ambos? ¿Se puede imponer un límite a la utilización de Google Classroom, por ejemplo?

Muchos países protegen en la OMC y diversos acuerdos comerciales a sus servicios públicos de las normativas de trato nacional y de acceso a los mercados por temas de interés nacional y soberanía. Pero, al ser un servicio digital, ¿pasa automáticamente a estar afectado por dichas normas impidiendo que un gobierno priorice una plataforma nacional por sobre una foránea?

Estos dilemas se empiezan a plantear en todos los sectores económicos, ya que la incorporación de cibernética es transversal a la economía en su conjunto. Pone en juego los derechos (como la educación y la salud) y la privatización indirecta de los servicios públicos. En efecto, la salud puede ser un servicio público no privatizado pero si el Estado subcontrata una empresa para que ésta se haga cargo de toda la telemedicina del Estado, entonces esta empresa tendrá los datos y podrá introducir una lógica comercial en el servicio, privatizando de manera indirecta la salud. Esto puede evitarse mediante la firma de un contrato que establezca las reglas mediante las cuales se presta el servicio. Pero, de firmarse este tipo de acuerdo de economía digital, limitará lo que pueda contener ese contrato.

La entrada de los productos digitales a los acuerdos de libre comercio implica la liberalización indirecta de todos los servicios producidos en la economía al presente, de forma indirecta, aun si están protegidos en el acuerdo. No solo eso, sino que también implica liberalizar servicios futuros que aún no han sido creados y que ni siquiera imaginamos.

Ejemplo

En el GATT (General Agreement on Tariffs and Trade) y el GATS (General Agreement on Trade in Services)⁸⁷, los gobiernos se tomaron el trabajo de permitir la discriminación de productos cuando se trata de compras públicas. Esto se debe a que muchas veces se usa este recurso para promover productos locales, sobre todo por cuestiones de desarrollo económico o motivos culturales. Si se aplican las normas de Trato Nacional y Nación más favorecida a los productos digitales sin hacer excepciones, los gobiernos no podrían, por ejemplo, tener preferencias por libros digitales o contenido educativo nacional para estudiantes de escuelas públicas.⁸⁸

¿Qué dice?

1. Las Partes no negarán la validez jurídica de una autenticación electrónica únicamente sobre la base de que el servicio se presta en forma electrónica.
2. Ninguna de las Partes adoptará ni mantendrá medidas que regulen la confianza electrónica y la servicios de autenticación que lo harían prohibir que las partes en una operación electrónica determinen de común acuerdo la métodos electrónicos para su transacción; o Impedir que las partes tengan la oportunidad de establecer antes de autoridades judiciales que su transacción electrónica cumple con los requisitos con respecto a la confianza.
3. No obstante lo dispuesto en el párrafo 2, una Parte podrá exigir que, para una determinada categoría de transacciones, el método de autenticación cumple ciertas normas de rendimiento o está certificado por un autoridad acreditada de acuerdo con su ley. Tales requisitos serán objetivos, *transparentes* y *no discriminatorios* y se referirá únicamente a las características específicas de la categoría de transacciones en cuestión.⁸⁹

¿Qué implica?

Esta cláusula es un ataque a la seguridad de los ciudadanos y consumidores.

Si bien esta cláusula en principio podría parecer lógica y certera, la realidad es que los sistemas informáticos de autenticación y firma electrónica, si bien son bastantes confiables, no están exentos de ataques y hackeos.

Lo cierto es que la fe ciega en los sistemas informáticos, juzgándolos como neutrales, confiables, seguros y veloces, ha hecho que las tecnologías comiencen a estar presentes en los ámbitos más diversos de la sociedad, aun cuando no son recomendados por los especialistas, como el caso del voto electrónico.

La firma electrónica puede no ser segura en muchos casos. Debería existir una vía de escape que permita al Estado regular que determinados contratos y acuerdos no puedan ser efectuados bajo documentos, firmas, o sellos electrónicos. Asimismo, existen diferentes estándares de seguridad. En informática pueden implementarse medidas sumamente difíciles de romper, como así también estándares laxos fácilmente sorteables. No siempre, pero si generalmente, a mayor seguridad, mayor costo.

Por este motivo, el artículo aclara que se pueden, en situaciones excepcionales, establecer estándares regulados por la autoridad de aplicación, pero el propio artículo aclara que estos deben ser objetivos, transparentes y no discriminatorios. El uso de este tipo de adjetivos sin definir qué se entiende por los mismos es clásico en los acuerdos de libre comercio, dejando a criterio de un tribunal ad hoc que generalmente se forma con los mismos abogados que defienden a las corporaciones, la libertad de entender qué es objetivo, transparente y no discriminatorio. Por este motivo es que los Estados generalmente no suelen hacer uso de este tipo de cláusulas por miedo a tener represalias y tener que afrontar costosísimos juicios producto del uso de las excepciones.

Ejemplo

Tal y como está redactado este artículo en la mayoría de los acuerdos, uno de los problemas que se presenta es que las partes del acuerdo sean las que decidan qué tecnología de autenticación usarán. Esto se ve claramente en el caso de Visa y Mastercard, dos empresas dominantes que pueden imponerse para establecer los estándares, que implementaron su “software antifraude” en su red comercial con el propósito declarado de garantizar que el sistema de pago fuera seguro. Sin embargo, la Federación Nacional de Minoristas de EE.UU. calificó el plan como una “casi estafa”, y en una impugnación legal se afirmó que “el sistema es menos un sistema para proteger los datos de las tarjetas de los clientes que un sistema para obtener ganancias para las empresas de tarjetas a través de multas y sanciones”⁹⁰. De hecho, se ha descubierto que muchas corporaciones son laxas con los datos de los consumidores, lo que lleva al robo de identidad y al fraude crediticio (las violaciones de Equifax de febrero y septiembre de 2017 son un ejemplo claro de esto), o a ataques cibernéticos a oleoductos y gasoductos (como le sucedió en abril de 2018 a Energy Services Group en EEUU y a Colonial Pipeline en Mayo 2021)⁹¹, y otros problemas que causan daños económicos a los consumidores y otros daños. Se hace evidente la necesidad de una regulación por parte del Estado -con directivas claras y precisas- y la presencia de una autoridad de aplicación que fije los estándares de seguridad de la tecnología utilizada para la autenticación, incluyendo la posibilidad de definir en qué casos no pueda utilizarse tecnología electrónica y deba recurrirse a otros métodos de autenticación, firmas y sellos.

PROTECCIÓN ONLINE DEL CONSUMIDOR

¿Qué dice?

1. Las Partes reconocen la importancia de adoptar y mantener medidas transparentes y eficaces para proteger a los consumidores, entre otras cosas, de las prácticas comerciales fraudulentas y engañosas cuando realizan transacciones de comercio electrónico. El consentimiento se definirá de conformidad con las leyes y reglamentos propios de cada Parte.
2. A tal fin, las Partes adoptarán o mantendrán medidas que contribuyan a la confianza de los consumidores, incluidas las medidas que proscriben las prácticas comerciales fraudulentas y engañosas. Tales medidas deberá, entre otras cosas, prever:
 - a. El derecho de los consumidores a una información clara y completa sobre el servicio y su proveedor;
 - b. La obligación de los comerciantes de actuar de buena fe y atenerse a las prácticas comerciales honestas, incluso en respuesta a las preguntas de los consumidores;
 - c. La prohibición de cobrar a los consumidores por servicios no solicitados o por un período en tiempo no autorizado por el consumidor;
 - d. Acceso a la reparación para que los consumidores reclamen sus derechos, incluso en lo que respecta a su derecho a recursos por servicios pagados y no prestados según lo acordado.
3. Las Partes reconocen la importancia de la cooperación entre sus respectivos organismos de protección del consumidor u otros órganos pertinentes sobre actividades relacionadas con el comercio electrónico con el fin de proteger a los consumidores y aumentar la confianza de los consumidores.⁹²

¿Qué implica?

Esta medida también forma parte de aquellas que, en principio, no están mal, pero que habrá que ver cómo se redactan y se aplican en los acuerdos ya que existen borradores como el TISA (Trade In Services Agreement), donde estos artículos son mucho más problemáticos.

En principio, la idea es correcta: proteger a los consumidores, darles una vía para reclamar, y demandar compensación en caso de que existan problemas. La cuestión aquí es si las agencias de protección al consumidor locales pierden jurisdicción en esta materia. Si bien se las menciona en el artículo diciendo que deben cooperar y que son importantes, no se les da jurisdicción para obrar en caso de que existan casos no resueltos por canales electrónicos. Esto puede ir en detrimento de los consumidores que al no encontrar respuesta de manera directa con la empresa, pueden recurrir a tribunales que no tengan poder para hacer que las empresas cumplan lo que deberían.

Ejemplo

Las corporaciones digitales han mostrado una falta de responsabilidad y compromiso en cuanto a garantizar la protección de sus consumidores. Todas las semanas se conocen noticias sobre filtración de datos e información personal y sensible de millones de usuarios y consumidores de todo el mundo de servicios prestados por grandes compañías de tecnología, ya sean proveedoras de servicios de mensajería, redes sociales o de transacciones económicas. Salen a la luz desde contraseñas, números de tarjetas de crédito, fotografías, etc. Además, los consumidores han presentado innumerables demandas después de descubrir que sus datos sobre el uso de productos o servicios, desde los auriculares Bose⁹³ hasta la gestión de correo electrónico⁹⁴ y los juguetes sexuales⁹⁵, se vendieron a otras empresas, generalmente sin el conocimiento o consentimiento del consumidor. Un reconocido escándalo internacional fue el de la empresa Facebook, cuando se supo que compartió de manera inapropiada los datos de 87 millones de usuarios con Cambridge Analytica⁹⁶ y que podría haber afectado el resultado de las elecciones estadounidenses en 2016. También existe evidencia de que afectó las elecciones de otros países de América latina como Argentina o Brasil⁹⁷. En los casos mencionados se hace evidente el problema al que se enfrentan los consumidores que no logran hacer valer sus derechos ante las corporaciones globales que no atienden sus demandas y la necesidad de que puedan contar con el rol institucional y legal de las agencias de protección de los consumidores locales, que tengan injerencia en esos casos para la protección de consumidores de sus países que quizás no logren resolver los problemas a través de canales electrónicos directos con las compañías.

MEDIDAS CONTRA COMUNICACIONES ELECTRÓNICAS NO SOLICITADAS

¿Qué dice?

1. Cada una de las Partes se esforzará por proteger eficazmente a los usuarios finales contra las comunicaciones comerciales directas no solicitadas. A tal fin, se aplicarán en particular los siguientes párrafos.
2. Cada una de las Partes se esforzará por garantizar que las personas físicas y jurídicas no envíen comunicaciones comerciales directas a los consumidores que no hayan dado su consentimiento.
3. No obstante lo dispuesto en el párrafo 2, las Partes permitirán que las personas físicas y jurídicas que han recogido, de acuerdo con las leyes y reglamentos propios de cada Parte, el contacto de un consumidor detalles en el contexto de la venta de un producto o un servicio, para enviar la comercialización directa comunicaciones a ese consumidor para sus propios productos o servicios similares.
4. Cada Parte se esforzará por asegurar que las comunicaciones comerciales directas sean claramente identificables como tales, revelen claramente en nombre de quién se hacen, y contengan la información necesaria que permita a los usuarios finales solicitar el cese de la actividad de forma gratuita y en cualquier momento.⁹⁸

¿Qué implica?

Aunque parece una medida contra el spam, en la práctica lo permitirá cuando un consumidor ya haya comprado bienes y servicios o cuando la empresa haya “recogido” los datos del consumidor legalmente. Es decir, que si te diste a conocer en la web como potencial consumidor interesado en determinado producto, automáticamente las empresas están autorizadas a enviarte la cantidad de publicidad que quieran. Esto es así porque las empresas de tecnología venden los datos de los potenciales consumidores a las empresas que proveen estos bienes, con lo cual no es necesario que le hayas dado el dato a una empresa en particular. A partir de que identifican tu perfil de consumidor, todas las empresas que compren dicha información podrán legalmente enviarte publicidad.

Ejemplo

Esta situación ya la vivimos hoy en día en Internet todos los usuarios de diversas redes sociales. La infinita cantidad de publicidad que se hace presente en nuestras computadoras ya se ha convertido en inmanejable. Más aún, si hacemos un esfuerzo futurista, a partir de la instalación de la red 5G y los hogares inteligentes, los electrodomésticos pasarán a tener pantallas para sugerirnos compras o avisarnos de fallas o advertencias automáticas. Estos mismos electrodomésticos muy probablemente estén conectados a nuestros teléfonos celulares, enviándonos información a los mismos. Nada impedirá que sea una constante catarata de publicidades en nuestros celulares, en nuestros hogares, cada vez que prendemos un electrodoméstico o nos acercamos a la heladera. Permitir que los Estados regulen esto a futuro puede defendernos frente a una potencial intoxicación de ofertas, publicidades, y consumismo desenfrenado.

¿Qué dice?

1. Cada una de las Partes reconoce que la protección de los datos personales y la privacidad es un derecho fundamental y que las normas elevadas a este respecto contribuyen a la confianza en la economía digital y al desarrollo del comercio.
2. Cada Parte podrá adoptar y mantener las salvaguardias que considere apropiadas para garantizar la protección de los datos personales y la privacidad, incluso mediante la adopción y aplicación de las normas para la transferencia transfronteriza de datos personales. Nada de este acuerdo afectará a la protección de los datos personales y la privacidad que ofrecen las respectivas salvaguardias de las partes.
3. Cada una de las Partes informará a la otra Parte sobre cualquier salvaguardia que adopte o mantenga de acuerdo con el párrafo 2.
4. A los efectos del presente acuerdo, se entenderá por “datos personales” toda información relativa a una persona física identificada o identificable.
5. Para mayor certeza, el Sistema de Tribunal de Inversiones no se aplica a las disposiciones en los Artículos 1 y 2.⁹⁹

¿Qué implica?

Si bien es completamente correcto darle la importancia que se merece la privacidad de los datos personales y no personales, existe una tendencia en diversos acuerdos de libre comercio a permitir analizar los estándares de seguridad y de protección de cada nación basándose en los estándares de otro país. Obviamente, y como suele ocurrir casi siempre, es muy caro y complejo para los países en vías de desarrollo cumplir con determinados estándares, sobre todo los europeos, que le permitan comerciar de igual a igual en la era digital.

La protección de datos y la privacidad se están volviendo vitales en esta nueva revolución industrial y los requerimientos de privacidad que demandan los tiempos que corren no siempre son los que están vigentes en las legislaciones nacionales. Esto no solo exige a los diversos países a actualizar su legislación y adaptarla a la europea, sino además modernizar sistemas e invertir en protección y seguridad con escasos recursos. En definitiva, elevar el estándar es bueno, y exigir una agenda en esa dirección es necesario, lo que hace falta es exigir pero brindando la ayuda necesaria para llegar a ese estándar deseado.

El artículo declara la importancia de trabajar en el aspecto pero no asegura compromisos en la materia ni determina cómo ayudar a los países menos desarrollados a tener la capacidad de garantizarlo. Es decir, no existe un compromiso real en la materia, sino más bien una declaración de interés. Lo que debería suceder es que se exija elevar estándares y se fijen normas mínimas internacionales que garanticen la privacidad y se otorgue a los países menos desarrollados recursos y ayuda mutua para llegar a esos estándares. Exigir sin dar herramientas puede resultar en una competencia desleal, donde los países que no logren alcanzar las normas establecidas queden fuera de juego. Esto en el mundo ya se ha visto en otras situaciones, como los estándares medioambientales: son necesarios y positivos, pero implican un alto costo a los países del sur global cuando no fueron ellos los responsables de la contaminación generada en el mundo mayormente. Se les exige alcanzar estándares de emisiones de CO2 cuando las naciones más desarrolladas lograron serlo contaminando

sin ningún tipo de control. Hoy los países en vías de desarrollo deben invertir en tecnologías más caras para alcanzar esos estándares internacionales. Eso mismo puede ocurrir con los datos si esta agenda empieza a encauzarse hacia la obligatoriedad. El camino correcto a seguir sea no incluir cláusulas de este tipo en acuerdos de libre comercio y si avanzar en una agenda de cooperación en otros organismos internacionales.

Cabe aclarar que existen normas sobre protección de datos en otros capítulos de los acuerdos de libre comercio, como en finanzas. Pero esos no fueron incluidos en el presente análisis.

Ejemplo

El Reglamento General de Protección de Datos de la Unión Europea es un ejemplo claro de regulación en materia de protección de datos personales desde la perspectiva de la protección de la privacidad como un derecho fundamental. En la norma se establece que para que la UE pueda transferir datos personales, su socio comercial debe pasar una “prueba de adecuación” para que los datos estén protegidos¹⁰⁰. Sin embargo, debido a que Estados Unidos no tiene una regulación única en materia de protección de datos, sino normas locales que difieren de estado a estado y entre industrias, la alternativa que existe para que pueda haber intercambios comerciales que involucren datos personales es que la UE permita que EEUU incluya en su acuerdo la posibilidad de reconocer que los regímenes voluntarios sean suficientes para cumplir con las disposiciones del acuerdo de libre comercio. Esta es una cuestión que no debería estar sujeta a adjudicación en un acuerdo comercial. Si se avanzara en este sentido, la decisión iría en contra del régimen de protección de datos y la privacidad de las personas de la UE para poder garantizar el intercambio comercial entre ambas partes. Sin embargo, como indican los antecedentes en materia ambiental, los regímenes voluntarios de cumplimiento corporativo no han logrado los objetivos para los que se implementaron¹⁰¹.

COMPRAS PÚBLICAS ELECTRÓNICAS

¿Qué dice?

1. Al realizar adquisiciones cubiertas de conformidad con el capítulo sobre contratos públicos la entidad adjudicadora deberá:
 - a. Velar por que la contratación se efectúe utilizando sistemas de tecnología de la información y programas informáticos, incluidos los relacionados con la autenticación y el cifrado de información, que están generalmente disponibles y son interoperables con otros sistemas y programas informáticos de tecnología de la información disponibles; y
 - b. Mantener mecanismos que garanticen la integridad de las solicitudes de participación y de las licitaciones, incluido el establecimiento del momento de la recepción y la prevención de acceso inapropiado.
2. Para cada una de las contrataciones abarcadas, la entidad adjudicadora publicará un aviso de las contrataciones previstas, al que se podrá acceder directamente y de forma gratuita por vía electrónica a través de un único punto de acceso. El anuncio de la contratación prevista permanecerá fácilmente accesible al público, por lo menos hasta la expiración del plazo indicado en el anuncio. Cada Parte enumerará el medio electrónico apropiado.
3. Para cada contratación abarcada, la entidad adjudicadora ofrecerá también sin demora una oferta sin restricciones y completa de acceso directo y gratuito por medios electrónicos a los documentos de contratación de la fecha de publicación de la notificación.¹⁰²

¿Qué implica?

Cuando un Estado realiza una licitación para que el sector privado participe de alguna inversión pública, normalmente decide las condiciones en las que se otorga la información y de qué manera se efectúa la licitación.

El artículo mencionado propone que las licitaciones sean efectuadas de una manera digital, con información accesible, gratuita y con estándares de ciberseguridad y formatos entregables que sean acordes a los que se consigan fácilmente en el mercado. Esto impone a los Estados, traspasar todas sus licitaciones al ámbito digital, facilitando la entrada de empresas multinacionales que no estén presentes en el país. Las limitaciones respecto al cobro de pliegos en la licitación, quitan un elemento recaudatorio de los Estados y son una facilidad más para las empresas. Más acceso a las compras públicas para competir, menor capacidad de poder beneficiar empresas nacionales a través de las mismas. A mayor competencia internacional, hay menos probabilidad de que empresas locales logren ganar la licitación.

Ejemplo

Dado que no se han propuesto excepciones en este párrafo, parece que la intención es que esto se aplique a todas las compras públicas, es decir a la compra de todos los bienes y servicios, a diferencia de lo planteado en otros acuerdos de libre comercio, como por ejemplo, el Tratado Trans Pacífico (TPP) que no cubre todos los bienes y servicios. Además, al no plantear un umbral mínimo en el valor, se pueden incluir contratos para hacer compras que, sin este acuerdo, podrían reservarse a micro, pequeñas o medianas empresas locales, y promover el desarrollo de una industria nacional (como pueden ser compras de productos de librería, por ejemplo).

RESPONSABILIDAD DE LOS INTERMEDIARIOS

¿Qué dice?

Responsabilidad de los prestadores de servicios intermediarios: simple transmisión

1. En el caso de la prestación de un servicio de la sociedad de la información consistente en transmitir, a través de una red de comunicación, información proporcionada por el destinatario del servicio o en proporcionar acceso a la red de comunicación, las partes se asegurarán de que el prestador de servicios no sea responsable de la información transmitida, siempre que el prestador de servicios:
 - a. no sea la fuente de la transmisión;
 - b. no seleccione al destinatario de la transmisión; y
 - c. seleccione y no modifica la información objeto de la transmisión.
2. Las actividades de transmisión y suministro de acceso a que se refiere el párrafo 1 comprenden el almacenamiento automático, intermedio y transitorio de la información transmitida, siempre que dicho almacenamiento se utilice exclusivamente para la realización de la transmisión a través de la red de transmisión.

Normas similares aplican a información en caché y almacenamiento permanente.¹⁰³

¿Qué implica?

En Internet existen los intermediarios de información como en cualquier otro sector económico. Facebook es un intermediario de la información que los usuarios postean. Netflix es un intermediario que lleva películas producidas en Hollywood (por mencionar algunas) a tu dispositivo electrónico.

En muchos casos, las plataformas intermediarias son utilizadas para cometer ilícitos. Por ejemplo, existen grupos de Facebook donde se comercializa fauna silvestre en Argentina, actividad que está penada por ley¹⁰⁴.

Este artículo reconoce que los intermediarios pueden ser utilizados para ilícitos. Por eso, los deslinda de responsabilidad respecto de los contenidos que transmiten a menos que el producto sea propio (una película producida por Netflix), o tenga la capacidad de seleccionar la información que va a transmitir o haya modificado activamente esa información. Este desligamiento de responsabilidad también incluye respecto del almacenamiento, mantención de información en caché y alojamiento de información. Un tribunal puede exigir prevención o terminar con una infracción. Normas parecidas aplican para almacenamiento en caché y alojamiento de información.

Deslindar de toda responsabilidad a los intermediarios es un riesgo cuando se tiene en cuenta que diversas plataformas son utilizadas para cometer delitos como trata de personas¹⁰⁵, tráfico de fauna silvestre, de armas o de drogas, pornografía de menores¹⁰⁶, entre otros delitos graves. Sin embargo, la forma ambigua en que está redactado el artículo no resuelve cuestiones fundamentales de responsabilidad y rendición de cuentas. Si se hiciera responsables a los intermediarios por todos los contenidos que circulen a través de sus plataformas, esto contemplaría a aquellos contenidos que podrían catalogarse, por ejemplo, como “discurso de odio” o “fake news”. En este caso, esto podría provocar que las plataformas ejerzan censura previa de contenidos sólo para evitar tener sanciones de algún tipo. Este tipo de medidas pueden vulnerar el derecho a la libertad de expresión de todos, en general, y de las minorías globales, en particular, que necesitan de espacios en plataformas como Facebook, Twitter o YouTube para hacer llegar sus reclamos, denuncias e información que no tienen espacio en los medios de comunicación masivos.

En este sentido, un artículo de estas características debería considerar no hacer responsables a los intermediarios en cuanto a los discursos que circulen en sus plataformas, para evitar vulnerar el derecho a la libertad de expresión, pero podría precisarse sobre qué delitos sí deberían tener obligaciones y responsabilidades dentro de sus espacios.

Ejemplo

Google y Facebook controlan la gran mayoría de la filtración y difusión de información y noticias, y sus algoritmos deciden qué información vemos y qué no. Su disposición a permitir que sus plataformas se utilicen para intervenir en procesos democráticos demuestra su colosal falta de interés en equilibrar su poder y sus responsabilidades. Uno de sus objetivos en las negociaciones comerciales digitales es asegurarse de que no se les pueda responsabilizar por el contenido generado por otros en su sitio, incluso si ese contenido fomenta la violencia, interfiere en las elecciones o causa otros daños, y es una fuente de ganancias para las corporaciones¹⁰⁷. Sin embargo, desde las sospechas de manipulación de desinformación en las redes sociales que surgieron a partir del resultado de las elecciones presidenciales de EEUU en 2016, que dieron ganador a Donald Trump, y durante todo su mandato hasta 2020 inclusive, en 2018 la FCC derogó la “Orden de Internet Abierta” y se sucedieron una serie de cuestionamientos a las plataformas¹⁰⁸ que llevaron a que tanto YouTube, Facebook como Twitter empiecen a ejercer una moderación de los contenidos de sus usuarios para evitar la propagación de “noticias falsas” y “discurso de odio”, con la consecuencia de baja de contenidos de organizaciones disidentes, discursos críticos¹⁰⁹ o grupos minoritarios.

¿Qué dice?

1. Las Partes no impondrán a los proveedores, una obligación general de supervisar la información que transmitan o almacenen, ni una obligación general de buscar activamente hechos o circunstancias que revelen actividades ilegales.
2. Las partes podrán establecer, para los prestadores de servicios de la sociedad de la información, la obligación de informar rápidamente a las autoridades públicas competentes de las actividades presuntamente ilícitas realizadas por los destinatarios de sus servicios o de la información presuntamente ilícita que éstos facilitarían o comunicarían a las autoridades competentes, a petición de éstas, información que permita identificar a los destinatarios de sus servicios con los que hayan concertado un acuerdo de acogida.¹¹⁰

¿Qué implica?

Este tema es muy debatido en distintos espacios políticos y sociales. ¿Cuán responsables son las plataformas de los contenidos que se agregan? ¿Queremos darles el poder de vigilancia respecto de qué se agrega y qué no? Hay opiniones encontradas respecto a este asunto. Algunos argumentan que, si tienen el poder, podrían utilizarlo para el bien y sacar los discursos de odio o de machismo de las redes sociales. Otros argumentan que con sacarlos no van a desaparecer de la sociedad, solo lo invisibilizan, y se le está dando a la plataforma un poder muy importante: el decir lo que está bien, y lo que está mal. ¿Qué pasará cuando se considere el ciberactivismo, el sindicalismo, o una determinada ideología política u económica, negativa y por ende susceptible de censura? ¿Queremos que empresas transnacionales tengan ese poder?

El artículo determina que las empresas no están obligadas a vigilar sus redes, pero no les prohíbe hacerlo y hasta dice que, si el gobierno lo pide, sí deben prestar ayuda. Claramente esto puede significar un ataque a la democracia y la libertad de expresión a futuro si un gobierno autoritario llega al poder.

ENDNOTES

- 1 Sai, Fabian Leonardo. 2019. Fragmentos de fragmentos: Vida psíquica, forma estética, potencia histórica. Revista Espectros, Año 5, Número 6. <http://espectros.com.ar/numero-6-fragmentos-de-fragmentos-vida-psiquica-forma-estetica-potencia-historica-leonardo-fabian-sai/>
- 2 Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism. Public Affairs.
- 3 Gurumurthy, Anita y Chami, Nandini. (2020) *The Intelligent Corporation Data and the digital economy* <https://longreads.tni.org/stateofpower/the-intelligent-corporation-data-and-the-digital-economy>
- 4 Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. Public Affairs.
- 5 https://en.wikipedia.org/wiki/Cambridge_Analytica
- 6 La idea de “manipulación directa”, como se quiso instalar desde los medios de comunicación al comienzo del escándalo de Cambridge Analytica, después de estudiarse el caso en profundidad, se comprobó que no existió tal y como se la describió (semejante a la teoría de la comunicación conocida como de la “aguja hipodérmica”) sino que lo que se notó fue que lo que se hacía era darle un último empujón a quienes ya tenían una clara tendencia de voto a favor de Trump (sobre todo porque los votantes republicanos suelen ser los que menos van a votar, a diferencia de los votantes demócratas). Ver: <https://carasycaretas.org.ar/2020/11/05/quien-toma-tus-decisiones/>
- 7 Strategy Lab, How Facebook Influences elections: The Great Hack Documentary. Disponible en: <https://strategylab.ca/how-facebook-influences-elections/>
- 8 Giving people ownership of their **personal data** (2018) Como el proyecto Decode, que plantea a la ciudad de Barcelona como ciudad inteligente pero con una lógica distinta donde el mercado no es el que determina las reglas de juego. Ver: <https://decodeproject.eu/>
- 9 Parminder, Jeet Singh. 2019. *Derechos en la sociedad de datos*. Fundación Friedrich Ebert Regional, Montevideo, Uruguay, <http://library.fes.de/pdf-files/bueros/uruguay/16201-20200529.pdf>
- 10 Scasserra, Sofía y Sai, Leonardo Fabián. 2020. *La cuestión de los Datos, Plusvalía de vida, bienes comunes y Estados inteligentes*. Fundación Friedrich Ebert Argentina. <http://www.fes.org.ar/public/LA%20CUESTI%C3%93N%20DE%20LOS%20DATOS.pdf>
- 11 Ha-Joon Chang, *Kicking Away the Ladder – Development Strategy in Historical Perspective*, Anthem Press, London, 2002
- 12 World Trade Organization, Electronic Commerce (1998) https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm
- 13 James, Deborah. 2020. *Digital trade Rules, A disastrous new constitution for the global economy written by and for Big Tech*. Rosa Luxemburg Stiftung. <https://www.rosalux.eu/en/article/1742.digital-trade-rules.html>
- 14 The New York Times (2020) The big tech lobbying europe. Disponible em: <https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html>
- 15 Corporate Europe Observatory (2020) Big Tech brings out the big guns in fight for future of EU tech regulation. Disponible em: <https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation>
- 16 No se incluye en el análisis cláusulas integradas en otros capítulos de los TLCs de la UE como finanzas o telecomunicación ni medidas de regulación doméstica o acceso a los mercados que también afectan a la economía digital.
- 17 Elaboración propia en base a los textos de los acuerdos mencionados. Donde dice PARCIAL, es porque se menciona la voluntad de seguir trabajando en la agenda a futuro pero no hay compromisos expresos respecto a la temática.
- 18 El acuerdo puede leerse acá: UE – CANADA (2018) <https://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/>
- 19 El acuerdo puede leerse acá: UE AND SINGAPORE (2018) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=961>
- 20 El acuerdo puede leerse acá: UE – VIETNAM (2018) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1437>
- 21 El acuerdo puede leerse acá: UE – MERCOSUR (2019) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=2048>
- 22 El acuerdo puede leerse acá: EU – JAPAN (2017) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684>
- 23 El acuerdo puede leerse acá: EU – MEXICO (2018) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1833>
- 24 World Trade Organization. 11th Ministerial conference – Buenos Aires (2017). Para ver la evolución de las excepciones, mirar el artículo de Sanya Reid Smith, *Some preliminary implications of WTO source code proposal*, disponible en <https://www.twn.my/MC11/briefings/BP4.pdf>
- 25 Comisión Europea/Cecilia Malmström/Comercio para todos. (2015) http://trade.ec.europa.eu/doclib/docs/2016/january/tradoc_154134.pdf

- 26 General Data Protection Regulation. (2016) <https://gdprinfo.eu/>
- 27 European Commission(2019) DG TRADE Strategic Plan (2016 – 2019). https://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154919.pdf
- 28 Klaus schwab.2016.World Economic Forum, Fourth Industrial Revolution. <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>
- 29 Comisión Europea. Estrategia europea de datos. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es
- 30 Adam Satariano and Matina Stevis-Gridneff (2020) *Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators.* *The New York Times.* <https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html>
- 31 Corporate Europe Observatory .(2020) Big Tech brings out the big guns in fight for future of EU tech regulation. <https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation>
- 32 El acuerdo puede leerse acá: The texts proposed by the EU for a Deep and Comprehensive Free Trade Area (DCFTA) with Tunisia (2016) <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1490>
- 33 El acuerdo puede leerse acá: EU – CHILE (2021) Commission releases its proposals and reports about progress. <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1793&title=EU-Chile-trade-talks-Commission-releases-its-proposals-and-reports-about-progress>
- 34 El acuerdo puede leerse acá: EU-Indonesia (2018) EU provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade Agreements. https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf
- 35 El acuerdo puede leerse acá: EU-Australia (2018) Trade Agreement negotiations <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1865>
- 36 EU-New Zealand. April 2021.El acuerdo puede leerse acá: <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1867>
- 37 El 2 de octubre de 2019, la UE inició las negociaciones con cinco socios de África Oriental y Meridional (la llamada ESA: Comoras, Madagascar, Mauricio, Seychelles y Zimbabue) para profundizar en el Acuerdo de Asociación Económica existente. El acuerdo incluye los países puede leerse acá: https://trade.ec.europa.eu/doclib/docs/2021/january/tradoc_159393.pdf a partir de la página 61.
- 38 El acuerdo puede leerse acá: Joint Statement on electronic commerce (2019) WTO. https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf
- 39 TWN Info Service on WTO and Trade Issues (Dec17/28). (2017) Third World Network. <https://www.twn.my/title2/wto.info/2017/ti171228.htm>
- 40 Para ver este tipo de argumentos, se puede visitar la página de la Semana del comercio Electrónico en UNCTAD <https://unctad.org/meeting/ecommerce-week-2019-digitalization-development> o el Foro Público de la OMC https://www.wto.org/english/forums_e/public_forum19_e/public_forum19_e.htm donde hay una diversidad de paneles defendiendo esta postura.
- 41 OECD ORG(2018) Bridging the digital divide. Include, upskill, innovate. <http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf>
- 42 Researchgate(2016) Gender Differences in Technology Usage—A Literature Review https://www.researchgate.net/publication/290475791_Gender_Differences_in_Technology_Usage-A_Literature_Review
- 43 Sofía Scasserra, 2016. E commerce, Future of labor and its impact on women. UNTREF. <https://itforchange.net/draft/e-commercer-future-of-labor-and-gender-gap.pdf>
UNCTAD (2021) Trade and Gender Linkages: An analysis of Least Developed Countries - Teaching Material on Trade and Gender: Module 4E (UNCTAD/DITC/2021/1). Disponible en <https://unctad.org/webflyer/trade-and-gender-linkages-analysis-least-developed-countries>
- 44 APWLD (2017) 164 women rights groups call on governments to reject the WTO declaration on womens economic empowerment. Disponible en: <http://apwld.org/press-release-164-womens-rights-groups-call-on-governments-to-reject-the-wto-declaration-on-womens-economic-empowerment/>
- 45 Estos argumentos pueden ser vistos en diversos paneles en, por ejemplo, el Foro Público de la OMC. https://www.wto.org/english/forums_e/public_forum18_e/pf18programme_e.htm
https://www.wto.org/english/forums_e/public_forum19_e/public_forum19_e.htm
- 46 https://unctad.org/system/files/non-official-document/eweek2018c01FED_en.pdf
- 47 Elaine Knutt,19/02/2021. WTO appoints Ngozi Okonjo-Iweala as new director general.Global,government Forum. <https://www.globalgovernmentforum.com/wto-appoints-ngozi-okonjo-iweala-as-new-director-general/>
- 48 Big Tech brings out the big guns in fight for future of EU tech regulation.12/2020. Corporate Europe Observatory. <https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation>
- 49 Huawei: UK government weighs up ban of Chinese firm's telecoms kit. July 2020. BBC. <https://www.bbc.com/news/technology-53306809>
- 50 Acuerdo de libre comercio que incluye una gran cantidad de países de la región de Asia y Oceanía.

- 51 Mauricio Claver Carone, 26/08/2020. Infobae. Candidato de Trump para el BID quiere limitar la influencia de China. <https://www.infobae.com/america/agencias/2020/08/26/candidato-de-trump-para-el-bid-quiere-limitar-influencia-china/>
- 52 Acuerdo de libre comercio entre EEUU y la UE que se firmó pero jamás se aprobó.
- 53 Continúan negociándose, pero la dirección neoliberal que va a adoptar la normativa ya está definida.
- 54 Se utilizó de modelo el artículo 1 de la propuesta de acuerdo de economía digital de la UE-Indonesia. July 2018. Disponible en https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf
- 55 Ver: Australian Government, Department of communication. Cloud Computing and privacy Consumer factsheet. Disponible en: <https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf>; Luiza Ch. Savage (2013), Trade Agreements, Privacy, and the Cloud, Disponible en: <http://www.macleans.ca/uncategorized/trade-agreements-privacy-and-the-cloud/>; ITI (2017) Data Localization Snapshot, Disponible en: <https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf>
- 56 Wikipedia. General Data Protection Regulation. Disponible en: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- 57 Comisión Europea (2020), Una Estrategia Europea de Datos. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>
- 58 Se utilizó de modelo el artículo 1 de la propuesta de acuerdo de economía digital de la UE-Indonesia. July 2018. Disponible en https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf
- 59 WEF (2020) Where data is stored could impact privacy, commerce and even national security and here is why. Disponible en: <https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/>
- 60 Global 5G: Rise of a Transformational Technolog. (2020). <https://www.5gamericas.org/global-5g-rise-of-a-transformational-technology/>
- 61 What Google does when a government requests your data. January 28, 2013. <https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/>
- 62 Colocation America (2020). The Future of Data Centers Renewable Energy. Colocation America. <https://www.colocationamerica.com/blog/renewable-energy-data-centers>
- 63 Technative (2020) Are Data Centres Helping The Economy? <https://technative.io/how-data-centres-are-helping-the-economies/>
- 64 Data Localization Snapshot.(2017) <https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf>
- 65 Inland revenue. Tax Technichal. Diverting personal services income by structuring revenue earning activities through a related entity such as a trading trust or a company: the circumstances when Inland Revenue will consider this arrangement is tax avoidance <http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html>
- 66 Wikipedia. Data heaven. Disponible en: https://en.wikipedia.org/wiki/Data_haven
- 67 Statista. (2021) Revenue from big data and business analytics worldwide from 2015 to 2022. Disponible en: <https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/>
- 68 CEPAL (2016) La nueva revolución digital: de la Internet del consumo a la Internet de la producción. Disponible en: <https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-Internet-consumo-la-Internet-la-produccion>
- 69 Nathan Reiff (2021) How Visa Makes Money. Disponible en: <https://www.investopedia.com/how-visa-makes-money-4799098>
- 70 Se utilizó de modelo el artículo X.9 de la propuesta de acuerdo de economía digital de la UE-Indonesia. July 2017. Disponible en https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf
- 71 Cody Cook, Rebecca Diamond, Jonathan V. Hall John A. List, and Paul Oyer. Mayo 2020. The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers <https://web.stanford.edu/~diamondr/UberPayGap.pdf>
- 72 O'Neil, Cathy. 2016. Weapons of math destruction. Crown Books.
- 73 Data USA. Porcentaje de profesionales en el sector IT por raza o etnia. <https://datausa.io/profile/soc/151251>
- 74 El concepto de código abierto, que en inglés se conoce como open source, se refiere a un tipo de software que se basa en un modelo de colaboración abierta, es decir que el código fuente se comparte abiertamente porque entiende que existen beneficios prácticos al compartir el código (por ejemplo, al haber más personas que estudian un código y trabajan en mejorarlo o en encontrarle vulnerabilidades, el resultado es un mejor código, por lo tanto, un mejor producto). El código abierto se diferencia del software libre en cuanto a que este último entiende la lógica de compartir el código desde cuestiones morales y filosóficas.

- 75 El código cerrado se llama así en contraposición al código abierto y se refiere al código fuente que no se encuentra disponible para cualquier usuario, es decir no se hace público. Esto es frecuente en empresas de desarrollo que tienen como valor y como recurso competitivo un sistema informático y que lo que hacen es vender licencias de uso de ese sistema, sin habilitar la posibilidad de que ningún competidor pueda estudiar el código y mejorarlo. Aquí puede leerse más sobre la diferencia entre ambos tipos de código: Guido Schryen (2009) Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. Disponible en: https://www.researchgate.net/publication/220891308_Security_of_Open_Source_and_Closed_Source_Software_An_Empirical_Comparison_of_Published_Vulnerabilities
- 76 For more information on this, it is highly recommended to read a paper done by Sanya Reid Smith available at (2017) <https://www.twn.my/MC11/briefings/BP4.pdf>
- 77 By Zeynep Tufekci ,2015. Volkswagen and the Era of Cheating Software. The New York Times <https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html>
- 78 Se utilizó de modelo el artículo X.3 de la propuesta de acuerdo de economía digital de la UE-Indonesia. September, 2017. Disponible en https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf
- 79 World Economic Forum. 5G Global Accelerator. <https://www.weforum.org/projects/5g-global-accelerator>
- 80 Rashmi Banga, June 2017 '*Rising Product Digitalisation and Losing Trade Competitiveness*', United Nations. Conference on Trade and Development.
- 81 Joseph Spanjers and Matthew Salomon (2017), '*Illicit Financial Flows in Developing Countries Large and Persistent*'; Global Financial Integrity, Washington, DC, 2017, www.gfintegrity.org/report/illicit-financial-flows-to-and-from-developing-countries-2005-2014/
- 82 Brian O'Keefe and Marty Jones (2015), 'Revenue Do-Si-Do: How Uber plays the tax shell game', Fortune Magazine, 22 October 2015, <http://fortune.com/2015/10/22/uber-tax-shell/>.
- 83 Rashmi Banga, June 2017. '*Rising Product Digitalisation and Losing Trade Competitiveness*', United Nations. Conference on Trade and Development.
- 84 Se utilizó de modelo una versión abreviada del artículo 45 del capítulo de servicios del acuerdo UE-Mercosur. 28 June 2019. Las itálicas son nuestras. Disponible en https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf
- 85 AirBNB Watch. Airbnb's Not So Sweet 16: Broken Neighborhoods. Disponible en: <https://airbnbwatch.org/airbnbs-not-sweet-16-broken-neighborhoods/>
- 86 Uber granted 18-month London license as judge overturns ban.CNBC (2020). <https://www.cnn.com/2020/09/28/uber-granted-temporary-london-license.html>
- 87 El GATT y el GATS son los acuerdos de comercio de bienes y servicios de la OMC donde se fijan las reglas comerciales multilaterales que rigen el comercio global.
- 88 "*Some of the implications of ecommerce proposals for government procurement*" by Sanya Reid Smith, Legal Advisor, Third World Network, 10 December 2017.
- 89 Se utilizó de modelo una versión abreviada del artículo 6 del capítulo de comercio digital del acuerdo UE-México. Abril 2018. Las itálicas son nuestras. Disponible en https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf
- 90 Zetter, K. (2012). Rare legal fight takes on credit card company security standard and fines. Retrieved from <https://www.wired.com/2012/01/pci-lawsuit/>
- 91 Naureen S. Malik, "Cyberattack" Wake-Up Call "Puts Pipeline Industry in Hot Seat", Bloomberg, (2018). Disponible en <https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat>
- 92 Se utilizó como modelo el artículo 49 del capítulo de servicios del acuerdo UE-Mercosur. 28 June 2019. Disponible en https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf
- 93 Jordan Graham, 20 April 2017 'Bose is accused of recording, selling audio information', Boston Herald.
- 94 Mike Isaac and Steve Lohr, (2017). '*Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data*', The New York Times.
- 95 Alex Hern, 14 March 2017 '*Vibrator maker ordered to pay out C\$4m for tracking users' sexual activity*', TheGuardian.
- 96 Issie Lapowsky, 17 March 2019. 'How Cambridge Analytica Sparked the Great Privacy Awakening', wired.com.
- 97 Cambridge Analytica in Latin America: What We Know So far. (2018).TeleSurHD <https://www.telesurenglish.net/analysis/Cambridge-Analytica-in-Latin-America-What-We-Know-So-far-20180322-0028.html>
- 98 Se utilizó de modelo el artículo 48 del capítulo de servicios del acuerdo UE-Mercosur. 28 June 2019. Disponible en https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf
- 99 Se utilizó de modelo el artículo 2 del capítulo de transferencia transfronteriza de datos del acuerdo UE-Indonesia. July 2018 Disponible en https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf
- 100 European Commission. (2016) Adequacy Decisions. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- 101 Laufer, W.S. (2013) Social Accountability and Corporate Greenwashing. *Journal of Business Ethics* 43, 253–261 (2003) doi:10.1023/A:1022962719299 y Koehler, D. (2007) The Effectiveness of Voluntary Environmental Programs—A Policy at a Crossroads? *Policy Studies Journal* Vol 35, Issue 4
- 102 Se utilizó de modelo una versión abreviada del artículo X.10 del capítulo de comercio digital del acuerdo UE-Indonesia. Disponible en https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf
- 103 Se utilizó una versión abreviada de los artículos 68, 69 y 70 del capítulo de comercio de servicios del acuerdo UE-Túnez. Abril 2016. Disponible en https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154487.pdf
- 104 Denunciaron a Facebook por la venta de animales protegidos.18/10/2017. *Diario Uno*. https://www.diariouno.com.ar/mendoza/denunciaron-a-facebook-por-la-venta-de-animales-prottegidos-10192017_H1fZQClz0M
- 105 La ONU advierte del aumento de trata de mujeres y niñas a través de las redes sociales en el contexto de la pandemia (2020). *Telemadrid*. <http://www.telemadrid.es/noticias/sociedad/ONU-advierte-sociales-contexto-pandemia-0-2286071375--20201112105748.html>
- 106 Christina M. Ward. (2020). Pedophilia is Alive on Facebook Report These Pages Immediately! <https://aninjusticemag.com/pedophilia-is-alive-on-facebook-report-these-pages-immediately-9ec2f3ea9296>
- 107 David McCabe and Ana Swanson (2019). 'U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators', *The New York Times*.
- 108 Rodrigo, Chris (2020). Tech CEOs clash with lawmakers in contentious hearing. <https://thehill.com/policy/technology/523268-tech-ceo-clash-with-lawmakers-in-contentious-hearing>
- 109 Jaime Altozano (2020). Los algoritmos de YouTube censuran un vídeo paródico de Pantomima Full sobre los negacionistas del coronavirus. *El diario .es* https://www.eldiario.es/tecnologia/youtube-censura-video-parodico-pantomima-full-negacionistas-coronavirus_1_6263109.html
- 110 Se utilizó una versión abreviada del artículo 71 del capítulo de comercio de servicios del acuerdo UE-Túnez. (2016). Disponible en https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154487.pdf



El Transnational Institute (TNI) es un instituto internacional de investigación e incidencia política que trabaja por un mundo más justo, democrático y sostenible. Durante más de 40 años, el TNI ha actuado como un punto de interconexión entre movimientos sociales, académicos y académicas comprometidos y responsables de políticas.

www.TNI.org